

2012

Protecting Personal Location Data for Private Aircraft Owners

Ashley Harris
Seton Hall Law

Follow this and additional works at: https://scholarship.shu.edu/student_scholarship

Recommended Citation

Harris, Ashley, "Protecting Personal Location Data for Private Aircraft Owners" (2012). *Law School Student Scholarship*. 42.
https://scholarship.shu.edu/student_scholarship/42

Protecting Personal Location Data for Private Aircraft Owners

INTRODUCTION

In the E-ZPass system alone, there are over twenty-one million vehicles with individual transponders to enable the expeditious payment of tolls on toll roads without cash.¹ In order for E-ZPass to work, the transponder unit, which is tied to the vehicle's license plate and owner's credit card information, is scanned whenever it passes through a toll collection site and the proper toll amount is billed or deducted.² Although the administrating agency, in this case E-ZPass, can identify which toll booths a vehicle has passed through (in fact it is sometimes necessary to know such information in order to charge the appropriate toll), that information is not available for the public to see.³ In fact, even law enforcement cannot access this information without a court order.⁴ Realistically, no reasonable person would expect a private vehicle's location information, namely the toll booths it accessed, to be available to anyone with an internet connection.

This situation is directly analogous to private aviation. The Federal Aviation Administration ("FAA") recently proposed a rule that would end an aircraft owner's ability to prevent his movement information from being released to the public.⁵ The program that currently allows owners to prevent this release is referred to as Block Aircraft Registration Request

¹ E-ZPass Interagency Group, *About Us*, E-ZPASS GROUP (2011), <http://www.e-zpassiag.com/about-us/overview>. The EZ Pass system is comprised of agencies from fourteen states in the Northeastern region of the United States, including the greater New York area. *List of electronic toll collection systems*, WIKIPEDIA (Feb. 25, 2012 10:24 PM), http://en.wikipedia.org/wiki/List_of_electronic_toll_collection_systems.

² *How does E-ZPass® work?*, E-ZPASS NEW YORK SERVICE CENTER (2008), <https://e-zpassny.com/en/about/howit.shtml>.

³ Dan Namowitz, *Expanded Aircraft-Tracking Plan Hit as Security Risk*, AIRCRAFT OWNERS AND PILOTS ASSOCIATION (Mar. 10, 2011), http://www.aopa.org/aircraft/articles/2011/110310expanded_aircraft_tracking_hit_as_security_risk.html.

⁴ *Most Common E-ZPass Myths*, PENNSYLVANIA TURNPIKE, http://www.paturnpike.com/aet_public/ezpass_myths.asp (emphasis added). The time stamps associated with a vehicle's location can only be used for purposes of assessing an accurate fine, and cannot be used to issue speeding tickets or other administrative enforcement violations. *Id.*

⁵ Access to Aircraft Situation Display (ASDI) and National Airspace System Status Information (NASSI), 76 Fed. Reg. 12,209 (proposed Mar. 4, 2011) [hereinafter *Proposed Rule*].

(“BARR”), by which private aircraft owners submit requests to have their information withheld from an otherwise automatic-disclosure data feed. The attempt by the FAA constituted a violation of personal privacy, and, fortunately, BARR has since been restored.⁶ However, BARR is insufficient in its privacy protection for some private aircraft owners due to its functioning as an “opt-out” system. Despite functioning to government and industry satisfaction for more than a decade, the BARR program should be reconfigured to an “opt-in” system to better align with prevailing protections of privacy.

This Note treats the movement and location information of private aircraft like that of private vehicles; it does not follow that the law should diminish the privacy of one group more than the other because it uses federal airspace as opposed to federally-funded highways. Part I describes the background and history of the BARR program, as well as describes the recent attempt by the FAA to change BARR’s applicability and the lawsuit that challenged this decision. Part II analyzes the privacy implications of BARR as it currently exists, in light of pre-existing federal law, namely the Privacy Act, the Fourth Amendment, and the relevant Freedom of Information Act (“FOIA”) provisions. This part will describe how a simple administrative change to the program from an “opt-out” to an “opt-in” policy would better reflect the government’s current treatment of an individual’s private information, and will suggest the alternative solution of removing the personally identifiable information from the released information as a means of protecting privacy. Ultimately, the applicable law and relevant considerations will lead to the conclusion that, while corporations are sufficiently protected under the current system, privacy rights afforded to individual people are likely being infringed by BARR and its policy of automatic disclosure.

⁶ See Background discussion *infra* Part I.

I. Background

In the National Airspace System of the United States, all aircraft must choose to fly using one of two regulation methods: Visual Flight Rules (“VFR”) or Instrument Flight Rules (“IFR”).⁷ VFR is flying at its most basic, where the pilot is primarily responsible for seeing and avoiding all other air traffic and any clouds.⁸ IFR is preferable because: it permits an aircraft to fly at altitudes over 18,000 feet,⁹ makes flight possible in most weather and through clouds,¹⁰ requires Air Traffic Control to be primarily responsible for separation from other aircraft,¹¹ and allows for easier Air Traffic Control tracking and coordination.¹² The vast majority of commercial flights (scheduled service provided by airlines) operate using IFR.¹³ In addition, many General Aviation (“GA”) users (i.e., non-scheduled, non-commercial flights¹⁴) prefer to fly under IFR because of the additional flexibility it offers. GA users who fly for transportation purposes do not want their travel limited by clouds and weather. Higher altitudes are also preferable because smoother air makes for less turbulence, increased fuel efficiency of the engines,¹⁵ and the absence of VFR traffic that is not permitted above 18,000 feet.¹⁶

⁷ 14 C.F.R. §§ 91.101-91.193 (providing for only two sets of rules under which aircraft may be operated). The Federal Aviation Regulations (“FARs”) set minimum weather conditions required to fly under VFR; any flights occurring during conditions that do not meet those minimums must use IFR if they wish to fly despite the less-than-ideal weather, unless as otherwise provided in the FARs. 14 C.F.R. § 91.155.

⁸ 14 C.F.R. § 91.113.

⁹ Class A airspace is defined as any airspace from 18,000 feet to 60,000 feet. 14 C.F.R. § 71.33 (2011). The FARs require any flight operating in Class A to be under IFR. 14 C.F.R. § 91.135.

¹⁰ *Id.*

¹¹ 14 C.F.R. § 91.173.

¹² Flight following is where ATC assigns a transponder code to an IFR flight, which allows for easy handoffs between controllers and easy tracking of the flight on the radar screens. This practice also makes it easier for Air Traffic Controllers to give in-flight traffic advisories to the pilots. 14 C.F.R. § 121.125.

¹³ Interview with Edward Bradley, Member & Pilot, Air Line Pilots Association, in Jersey City, N.J. (Oct. 12, 2011).

¹⁴ “The Federal Aviation Administration defines general aviation as all flights that are not conducted by the military or the scheduled airlines.” *What is Business Aviation?*, NATIONAL BUSINESS AVIATION ASSOCIATION (2012), <http://www.nbaa.org/business-aviation/>.

¹⁵ See Bradley, *supra* note 13

¹⁶ *Id.*; see also 14 C.F.R. § 91.135.

In order to fly using IFR, the pilot must file an official flight plan prior to departure.¹⁷ The information typically contained in a flight plan includes the origin and destination airports; anticipated altitude and airspeed; expected departure and arrival time; planned route utilizing navigational aids; fuel usage; alternate destinations if the weather is questionable; pilot's name(s); and number of people on board.¹⁸ The Federal Aviation Administration ("FAA") collects this data and uses it for safety and airspace management purposes. Combined with radar, this data allows the FAA to monitor the progress of flights in real time through a network called Aircraft Situation Display ("ASDI").¹⁹

In addition to using ASDI for air traffic control, the FAA also shares it with public and private entities upon request.²⁰ This system provides a real-time feed of the nation's airspace to Class One subscribers such as commercial airlines and near-real time feed (meaning typically a delay of about five minutes from current airspace positions) to Class Two subscribers.²¹ This relationship between the FAA and the subscribers is governed by a Memorandum of Agreement ("MOA"), entered into individually with each subscriber.²² Any member of the public can request to become a Class Two subscriber and receive the near-real time stream of the present location of airborne aircraft.²³ The most common Class Two subscribers are commercial websites, such as www.FlightAware.com ("FlightAware"),²⁴ who then make that information available to anyone with an internet connection. The practical result of this system is that all of

¹⁷ 14 C.F.R. § 91.169; *see also* 14 C.F.R. § 91.153 (listing the requirements for a VFR flight plan, if the pilot were to opt to file one, even though it is not required to do so).

¹⁸ 14 C.F.R. § 91.169.

¹⁹ *Block Aviation Registration Request (BARR) Program*, NATIONAL BUSINESS AVIATION ASSOCIATION (May 9, 2011), <http://www.nbaa.org/ops/security/barr/background/> [hereinafter *Background of the BARR Program*].

²⁰ *Id.*

²¹ *Proposed Rule*, *supra* note 5 at 12,210.

²² *Background of the BARR Program*, *supra* note 19.

²³ *Memorandum of Agreement, Version 1.4*, FEDERAL AVIATION ADMINISTRATION 2, http://www.fly.faa.gov/ASDI/asdidocs/ASDI_MOA_Ver_1.4_07212011.pdf.

²⁴ *Home Page*, FLIGHTAWARE (2012), www.flightaware.com.

the flight plan data mentioned above can be seen by the general public on various websites with present locations tracked in near-real time.²⁵ In addition, websites like FlightAware also save the data to create a comprehensive history of a particular aircraft, airport, or frequent flight.²⁶

Very quickly after this data became available to the public over the internet, both industry users and government officials recognized the privacy or confidentiality issue for GA owners and operators posed by the dissemination of data.²⁷ In response to this concern, Congress included language in the Wendell H. Ford Aviation Investment and Reform Act for the 21st Century (“AIR 21”) that required all ASDI subscribers to have the capability to selectively block the display of information for certain aircraft requested by the FAA.²⁸ In order for an aircraft owner to prevent his flight data from being released, he had to submit a request to the National Business Aviation Association (“NBAA”), which compiled a list of requests and sent monthly updates to the FAA.²⁹ This list would become the “blocked list” of aircraft whose movements would not be visible to the public, by request of the FAA as provided for in the MOA.³⁰ Under this program, known as Block Aircraft Registration Request (“BARR”), only non-commercial flights may submit requests to have their travel information protected. BARR greatly appealed to all types of GA flights, ranging from businesses or corporations trying to keep secret a CEO’s travels, to aircraft-owning celebrities looking for a paparazzi-free getaway, to individual citizens who simply did want others to be able to track their constant location.³¹

²⁵ *Frequently Asked Questions*, FLIGHTAWARE (2012), <http://flightaware.com/about/faq.rvt>.

²⁶ *Id.*

²⁷ *Background of the BARR Program*, *supra* note 19.

²⁸ Wendell H. Ford Aviation Investment and Reform Act for the 21st Century, Pub. L. No. 106-181, § 729, 114 Stat. 168 (Apr. 5, 2000) (codified at 49 U.S.C. §44103 *note*).

²⁹ *Background of the BARR Program*, *supra* note 19.

³⁰ *Id.*

³¹ Chad Trautvetter, *AIN Blog: FAA Should Leave BARR Alone*, AIN ONLINE (Apr. 15, 2011), <http://www.ainonline.com/?q=aviation-news/blogs/ain-blog-faa-should-leave-barr-alone>.

The BARR program operated effectively for fourteen years through collaboration with the NBAA, providing ADSI subscribers with access to flight tracking information, but also allowing for the privacy of those who requested it to be protected.³² In March 2011, the FAA issued a Notice of Proposed Modification to the FAA/Subscriber MOA (“proposed rule”) in the Federal Register, which described how it intended to modify the MOA with ASDI subscribers in order to change its interpretation of what it would “request” to be blocked.³³ The agency proposed that it would no longer accept requests for an undisclosed or generalized reason; rather, it would permit an aircraft to be blocked only if the owner annually submitted an approved Valid Security Concern.³⁴ This change effectively reversed FAA recognition that privacy rights were implicated by the ASDI program; in fact, the FAA specifically noted as much in the proposal.³⁵ After a legally sufficient comment period and time for revisions based on those comments, the FAA issued its Notice of Modification to the FAA/Subscriber MOA (“final rule”) on June 3, 2011, which had the effect of making the proposed regulation final.³⁶ The final rule took effect August 2, 2011, sixty days after its issuance in the Federal Register.³⁷

The comments to the proposed rule were very one-sided. Of the 621 comments that were submitted, only twenty expressed complete support for the proposal.³⁸ Out of these twenty, some do not specify a reason for their support, and only a handful appear to come from someone familiar with the industry.³⁹ The main reasons given in support of the proposal was to limit a corporation’s ability to deceitfully use its aircraft and to increase public oversight and monitoring

³² *Background of the BARR Program*, *supra* note 19.

³³ *Proposed Rule*, *supra* note 5 at 12,210.

³⁴ *Id.*

³⁵ *Id.*

³⁶ Access to Aircraft Situation Display (ASDI) and National Airspace System Status Information (NASSI), 76 Fed. Reg. 32,258 (June 3, 2011) [hereinafter *Final Rule*].

³⁷ *Id.*

³⁸ See Comments to Access to Aircraft Situation Display (ASDI) and National Airspace System Status Information (NASSI), 76 Fed. Reg. 12,209 (proposed Mar. 4, 2011) [hereinafter *Comments*].

³⁹ *Id.*

of corporate aviation.⁴⁰ The opponents of the regulation, in addition to being significantly more numerous, provided considerably more in-depth responses and reasoning that examined relevant factors on both sides of the issue.⁴¹ Despite varying significantly in wording and validity, some of the bases for opposing the proposed rule included: procedural insufficiency; additional administrative burden on both industry and FAA; the public benefit derived against the privacy concerns; the lack of government activity actually being disclosed; loss of competition; detriment to safety; terrorism; disparate treatment as opposed to automobiles; and the precedent this change would set.⁴² FlightAware.com, one of the more prominent ASDI subscribers, in fact opposed the proposed change, stating that “[a]lthough the proposed change would stand to financially benefit FlightAware, we oppose the change on the basis that it is misguided, overly broad and simplified, and would negatively impact the transportation sector as well as the US economy at large.”⁴³

Since President Obama took office, there has been an influx of open-government initiatives.⁴⁴ Spanning executive agencies and offices all the way up to the President, the current

⁴⁰ *Id.*

⁴¹ *Id.*

⁴² *Id.*

⁴³ Comment to Access to Aircraft Situation Display (ASDI) and National Airspace System Status Information (NASSI), 76 Fed. Reg. 12,209 (proposed Mar. 4, 2011) (comment of FlightAware).

⁴⁴ *See generally Transparency and Open Government*, Memorandum from President Barack Obama for the Heads of Executive Departments and Agencies (Jan. 21, 2009), available at http://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment; *Freedom of Information Act*, Memorandum from President Barack Obama for the Heads of Executive Departments and Agencies (Jan. 21, 2009), available at http://www.whitehouse.gov/the_press_office/FreedomofInformationAct; *Open Government Plan*, UNITED STATES DEPARTMENT OF TRANSPORTATION (Apr. 7, 2010), available at http://www.dot.gov/open/pdf/DOT_Open_Gov_Plan_V1.2_06252010.pdf; *Open Government Directive*, Memorandum from Office of Management and Budget for the Heads of Executive Departments and Agencies (Dec. 8, 2009), available at http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf; *The Freedom of Information Act*, Memorandum from the Att’y Gen. for Heads of Executive Departments and Agencies (Mar. 19, 2009), available at <http://www.justice.gov/ag/foia-memo-march2009.pdf>. Also, the OPEN Government Act of 2007 was passed with the same intent, however it was passed and enacted prior to President Obama taking office. Openness Promotes Effectiveness in our National Government Act of 2007. Pub. L. No. 110-175, 121 Stat. 2524 (2007).

administration places high importance on disclosure of government information.⁴⁵ In fact, a Presidential Memo regarding FOIA instructs agencies to “take affirmative steps to make information public,” and that “[t]hey should not wait for specific requests from the public” to do so.⁴⁶ Based on this administrative setting, the FAA claimed in its Final Notice that it decided to take this action to be more aligned with the prevailing executive policy.⁴⁷

An additional trigger brought the issue of BARR’s “secrecy” to the attention of the FAA: a recent FOIA request that led to a “reverse-FOIA” legal challenge to prevent the requested information from being disclosed.⁴⁸ While a typical FOIA action is brought by a non-governmental party seeking to compel the government to disclose information, a reverse-FOIA action is brought by an entity seeking to enjoin the government from making a disclosure.⁴⁹ In this case, a media outlet requested a list of the aircraft tail numbers whose movements were being blocked by BARR.⁵⁰ The outlet, a “non-profit news organization[,]” claimed, as the basis for its FOIA request, an “interest in investigating and reporting on politicians’ use of private aircraft, the use of private jets by corporations that have accepted taxpayer dollars from the U.S. government during the recent recession, and the environmental impact of aircraft use.”⁵¹ Upon notice from the FAA that it was preparing to release the block list, the NBAA instituted the reverse-FOIA action to prevent the release.⁵² Finding that no exclusion under FOIA applied to

⁴⁵ *Id.*

⁴⁶ Freedom of Information Act, Memorandum for the Heads of Executive Departments and Agencies, 74 Fed. Reg. 4683, Jan. 21, 2009, *available at* <http://federalregister.gov/a/E9-1773>.

⁴⁷ *Proposed Rule*, *supra* note 5 at 12,210; *Final Rule*, *supra* note 26 at 32,260-61.

⁴⁸ *See Nat’l Bus. Aviation Ass’n v. Fed. Aviation Admin.* (“NBAA v. FAA”), 686 F. Supp. 2d 80 (D.D.C. 2010).

⁴⁹ “A person whose information is about to be disclosed pursuant to a FOIA request may file a reverse-FOIA action and seek to enjoin the Government from disclosing it.” *Id.* at 84, *quoting* *Canadian Commercial Corp. v. Dep’t of Air Force*, 514 F.3d 37, 39 (D.C. Cir. 2008) (internal quotations omitted).

⁵⁰ *NBAA v. FAA*, 686 F. Supp. 2d at 84.

⁵¹ *Id.* at 83 n.5.

⁵² *Id.* at 83-84.

the subject information, the District Court of D.C. mandated the FAA release the list.⁵³ This case, combined with at least one other isolated incident of corporate CEO travel being made public,⁵⁴ generated negative publicity for the FAA,⁵⁵ ultimately causing it to initiate a change to BARR.

The change to BARR that disallowed the blocking of movement information without a specific, verifiable security concern was vehemently opposed by various industry groups. The NBAA, in conjunction with the Aircraft Owner's and Pilot's Association (AOPA) filed a lawsuit challenging the procedural sufficiency of the Final Rule,⁵⁶ with a supporting amicus curiae brief filed by the Experimental Aircraft Association.⁵⁷ The FAA had already filed its reply brief and a date for oral arguments had been set for December 2, 2011, when the lawsuit was rendered moot.⁵⁸ On October 31, 2011,⁵⁹ Congress passed the Consolidated and Further Continuing Appropriations Act of 2012, which included a provision that effectively returned BARR to its original operation.⁶⁰ This congressional action came after numerous other bills had been introduced into both the House and Senate in order to explicitly overturn the FAA's action.⁶¹

⁵³ *Id.* at 87. However, the request was only for the *list of aircraft* that were being blocked; it did not request any movement information about the aircraft, a distinction that the court noted in its opinion.

⁵⁴ When the recent economic crisis hit the automobile industry in 2009, the CEOs of GM, Chrysler, and Ford flew on their corporate jets to Washington D.C. in order to ask Congress for bailout money. This seemingly fiscally irresponsible act caused outcry among taxpayers. As a result of the intensified scrutiny of how it was using its corporate jet, GM submitted the tail number of its aircraft to have its movements blocked from public view. This act of requesting to be blocked, in itself, also spawned media attention and brought the BARR program into the public spotlight, where it was immediately viewed in a negative light due to the surrounding circumstances. John Hughes & Elliot Blair Smith, *GM Asks U.S. FAA to Bar Public Tracking of Leased Corporate Jet*, BLOOMBERG (Nov. 27, 2008), <http://www.bloomberg.com/apps/news?pid=newsarchive&sid=afKerH3i.2Y>.

⁵⁵ *See, e.g., Id.*; Michael Grabell, *Business Jet Group Tries to Block FOIA Request*, PROPUBLICA (June 17, 2009), <http://www.propublica.org/article/business-jet-group-tries-to-block-foia-request-616>.

⁵⁶ Nat'l Bus. Aviation Ass'n v. Fed. Aviation Admin., No. 11-1241 (D.C. Cir. filed Aug. 29, 2011).

⁵⁷ Brief for Experimental Aircraft Ass'n, Inc. as Amicus Curiae Supporting Petitioners, Nat'l Bus. Aviation Ass'n v. Fed. Aviation Admin., No. 11-1241 (D.C. Cir. filed Aug. 29, 2011).

⁵⁸ *See* Consolidated and Further Continuing Appropriations Act, 2012, Pub. L. No. 112-55, § 119A, 125 Stat. 552 (2011).

⁵⁹ Signed by President Obama into law on November 17, 2011.

⁶⁰ Consolidated and Further Continuing Appropriations Act, 2012, *supra* note 56. The relevant paragraph actually prohibits the FAA from using any of its appropriated funds for programs that purport to limit the ability of individual aircraft owners to request that their privacy be protected. *Id.*

⁶¹ *See generally* FAA Reauthorization Act of 2011, H.R. 658, 112th Cong. § 817 (2011) (BARR preservation was built in as part of the reauthorization); BARR Preservation Act of 2011, S. 1477, 112th Cong. (2011); BARR

While restoring BARR to its status prior to the FAA's change is definitely a step towards better protection of personal privacy, it is not enough. The FAA should amend BARR in the opposite direction: rather than permitting aircraft owners to submit requests to block their movement information, it should automatically block all private movement information until the owner has submitted a request to have it publicly displayed. Alternatively, the same governmental disclosure interests in disclosing all the data would be achieved by the less-intrusive system of releasing movement information without the tail number attached.

People do not need a specific reason to want their personal information to remain private. This fundamental principle is reflected in BARR's operation: general aviation users who wish to have their flight data blocked from public view can submit merely a bare-bones request to be blocked without giving a supporting reason.⁶² While it is concededly easy to have the information blocked or removed from public display, the fact that disclosure is automatic until a request is submitted is the problem. Private aircraft owners could suddenly encounter a situation in which they would like the flight data to not be available online. Unfortunately for this owner, the block request process takes a month or more to become effective,⁶³ and any privacy, security, or safety concerns that might arise with little notice will go unaddressed.

II. Analysis

Individual owners of aircraft should be entitled to privacy in their flight movements the same way drivers are protected from release of their tollbooth data. There are multiple federal laws with which the BARR program could be found incompatible. This Part will focus on the Privacy Act, FOIA, and a possible connection to the Fourth Amendment. When assessing

Preservation Act of 2011, H.R. 2897, 112th Cong. (2011). Although not identical in wording to the provision in the FAA Reauthorization Act, the BARR Preservation Act in both Houses was very similar and would have had the same ultimate practical effect.

⁶² See *Background of the BARR Program*, *supra* note 19.

⁶³ *Background of the BARR Program*, *supra* note 19.

whether any of these laws are implicated by BARR, it is important to consider to whom the federal laws extend protection. For example, the Privacy Act protects government-held personal information of individual people, but whether similar protections apply to corporate entities is less clear.⁶⁴ Therefore, this Part will address the applicability of each of these laws in addition to the type of aircraft owner that would be entitled to possible protection.

A. The Privacy Act

The Privacy Act was enacted for the purpose of protecting personal records that are either collected and/or maintained by the government from being released to the public.⁶⁵ At its most basic function, the Privacy Act serves to “provide certain safeguards for an individual against an invasion of personal privacy.”⁶⁶ In passing the Act, Congress recognized that privacy is a fundamental basis of our society, and individuals should be automatically entitled to protection until a prevailing cause mandates otherwise.⁶⁷ The Privacy Act defines “record” as “any item, collection, or grouping of information about an individual that is maintained by an agency,”⁶⁸ and protects records from disclosure to any person or other agency without prior consent from the individual about whom the record is maintained.⁶⁹ Even from just the plain language of the Act, the flight movement data clearly fit the definition of “record,” and thus should be entitled to protection. Information supplied on a flight plan by an aircraft owner to the FAA, and the compilation of that movement data, should be considered a “grouping” of information sufficiently “about an individual.”⁷⁰

⁶⁴ See discussion of Privacy Act *infra* Part IIA.

⁶⁵ Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (1974).

⁶⁶ Privacy Act of 1974, Pub. L. No. 93-579, § 2(b), 88 Stat. 1896 (1974).

⁶⁷ *Id.*

⁶⁸ 5 U.S.C. § 552a(a)(4) (2010).

⁶⁹ 5 U.S.C. § 552a(b).

⁷⁰ See *id.*

Any remaining doubt about whether the aircraft movement data is sufficiently “about” the aircraft owner should be dispelled by appreciating how simple it is to connect the aircraft tail number with its owner. The FAA Aircraft Registry, a database of all aircraft registered in the United States, is available, free of charge, on the FAA website.⁷¹ The database can be searched by tail number, owner, state of registration, and more.⁷² Effectively, anyone who already has the tail number of an aircraft can use this website to find the owner and vice versa.⁷³ Therefore, any aircraft data that can be retrieved using the tail number should also be considered to be a “record” of the owner under the Privacy Act.

The Privacy Act protects “system[s] of records,”⁷⁴ which include records that can be retrieved based on the individual’s name or any identifying number assigned to the individual.⁷⁵ This data should be protected from disclosure is because the tail number of the aircraft, being registered in the name of the owner (and with that registration information being so readily ascertainable online), should be considered an identifying number assigned to that individual, the owner. Because the movement data can be retrieved based on a tail number, which is for all intents and purposes equivalent to the owner’s name,⁷⁶ the ASD database containing the movement information should be considered a “system of records” and used within the Privacy Act.

In its Proposed Rule and Final Rule, the FAA claimed that Privacy Act does not cover the disclosure that the intended modification to the MOA would have made while offering very little

⁷¹ *FAA Registry, Aircraft Inquiry*, FEDERAL AVIATION ADMINISTRATION (last visited Mar. 6, 2012), <http://registry.faa.gov/aircraftinquiry/>.

⁷² *Id.* Other search parameters include the make and model of the aircraft, county or country of registration, serial number of the aircraft, engine registration number, and recent registrations via the aircraft manufacturer.

⁷³ *Id.*

⁷⁴ 5 U.S.C. § 552a(b).

⁷⁵ 5 U.S.C. § 552a(a)(4).

⁷⁶ See *FAA Registry*, *supra* notes 69-70.

explanation as to why this is so.⁷⁷ The Final Rule cited to the relevant part of the MOA by simply quoting “[t]he protection of such information is not covered under the Privacy Act....”⁷⁸ However, neither the Final Rule nor the MOA describe why this is true.

The only explanation offered in the Final Rule is that “[a]ircraft registration information (including aircraft type, current status and ownership of aircraft, registration number, etc.) is in a System of Records protected by the Privacy Act.”⁷⁹ This reference to the Privacy Act seems to suggest that this database is permitted to be disclosed by an exception to the Privacy Act. However, the System Notice DOT/FAA 801 being referred to by the FAA does not encompass, or even contemplate, the movement data that is the subject of the current challenge.⁸⁰ Rather, as required in the Privacy Act,⁸¹ the System Notice merely registers and delineates the scope and purpose of the FAA’s Aircraft Registry database,⁸² which is limited to the aircraft owner, description, registration, and airworthiness specifications.⁸³ This Aircraft Registry is a separate database that makes public registration information pertaining to all civil aircraft registered in the United States,⁸⁴ and should not be confused with the movement and location information presently at issue. In essence, it appears that the FAA assumed disclosure is not precluded by the Privacy Act by claiming reliance on a separate, inapplicable exemption from the Act.⁸⁵ Although the FAA may have been mistaken, as a practical matter, however, a challenge to the disclosure of movement information under the Privacy Act never would have needed to happen, as any

⁷⁷ *Proposed Rule*, *supra* note 5 at 12,210; *Final Rule*, *supra* note 26 at 32,263.

⁷⁸ *Final Rule*, *supra* note 26 at 32,263. It should be noted that the MOA is not legal authority in itself, as it is just an agreement between the FAA and the direct subscribers to the ASD information. The FAA was also the original drafter of the MOA, so it effectively cited itself for support in its Final Rule.

⁷⁹ *Id.*

⁸⁰ System of Records, DOT/FAA 801, 65 Fed. Reg. 19,518 (Apr. 11, 2000) (merely providing for the storage of records pertaining to aircraft owners and registration).

⁸¹ 5 U.S.C. § 552a(b).

⁸² *See* System of Records, *supra* note 78.

⁸³ *See FAA Registry*, *supra* notes 69-70.

⁸⁴ *Id.*

⁸⁵ *See Final Rule*, *supra* note 26 at 32,263.

individual who is adversely affected by a disclosure had the much simpler and cheaper option of submitting a BARR request.

In a Preliminary Report on modern-day privacy, the Federal Trade Commission noted that location-based information “raises important privacy concerns” because, for example, “the retention of location information about a consumer’s visits to a doctor’s office or hospital over time could reveal something about that consumer’s health that would otherwise be private.”⁸⁶ This language shows regulatory recognition of an interest in keeping the sum total of one’s locations and destinations a secret if one so chooses. This principle should also be applied to location information that can be ascertained from making flight data available to the public.

Proponents of the modification to BARR pointed to the fact that the flight data to be disclosed stops tracking the individual’s movement at the airport, and it is impossible to tell where any passengers go from there. However, the only difference between the example in the - FTC report and the ASDI flight data is the specificity. If an aircraft flies into an airport, an observer does not necessarily know where the passenger’s final destination is, as the tracking ends as the passenger leaves the aircraft at the airport instead of at the doctor’s office. Realistically, however, coupling the airport destination information with other known information may make it clear where the passenger is headed after deplaning. Without knowing the destination, there would be no way of discerning the information.

Although at first it may seem speculative to actually be able to draw these connections, the Wall Street Journal has already demonstrated, with much bravado, that it can be done.⁸⁷ For

⁸⁶ FED. TRADE COMM’N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS 47 (Dec. 2010).

⁸⁷ The Wall Street Journal published an article that included specific aircraft owners, names of individuals, the number of flights to particular destinations, and estimates of the costs of flights. Mark Maremont & Tom McGinty, *For the Highest Fliers, New Scrutiny*, THE WALL STREET JOURNAL (May 21, 2011), available at <http://m.india.wsj.com/s/4150/388?articleId=SB10001424052748703551304576260870733410758&fullStory=fullStory>. The authors also created an interactive webpage on the WSJ website to aid readers in searching for a particular

example, by simply knowing that actor John Travolta is a member of the Church of Scientology and being able to ascertain that his private aircraft was flown repeatedly to Clearwater, Florida (the headquarters of the Church), the Wall Street Journal article came to the conclusion that Travolta visited the Church headquarters 111 times in four years.⁸⁸

Even if the records were not subject to protection under the Privacy Act, existing federal laws indicate an overwhelming public policy interest to the contrary. The existence of the Privacy Act (section 552a), conveniently next to FOIA (section 552), shows Congress has recognized a distinction between “[p]ublic information[,] agency rules, opinions, orders, records, and proceedings”⁸⁹ and “[r]ecords maintained on individuals,”⁹⁰ and has chosen to protect the latter.⁹¹ There have been many other statutes enacted in various regulatory fields that show similar Congressional intent.⁹² When read together with this myriad of other statutes, the Privacy Act shows Congress’ expressed interest in protecting personal data from government disclosure, to which BARR’s opt-out system barely pays respect.

On the contrary, altering BARR to allow disclosure only when a party opts-in to the disclosure seems much more in line with the congressional intention, and will better protect

aircraft or owner and their flight histories. *Jet Tracker*, THE WALL STREET JOURNAL (last accessed March 6, 2012), <http://projects.wsj.com/jetracker/#a=&d=&e=2011-01-01&m=grouped&o=&p=0&s=2007-01-01&sort=d&t=&v=table>. This website was created based on data obtained from the FAA’s ASDI system.

⁸⁸ *Id.*

⁸⁹ 5 U.S.C. § 552 (2009).

⁹⁰ 5 U.S.C. § 552a.

⁹¹ *See generally* 5 U.S.C. § 552; 5 U.S.C. § 552a.

⁹² *See* Comment to Access to Aircraft Situation Display (ASDI) and National Airspace System Status Information (NASSI), 76 Fed. Reg. 12,209 (proposed Mar. 4, 2011) (comment of the National Business Aviation Association) (citing the Telemarketing and Consumer Fraud and Abuse Prevention Act, the Fair Credit Reporting Act, the Family Educational Rights and Privacy Act, the Telephone Consumer Protection Act of 1991, the Internal Revenue Service confidentiality requirements in 26 U.S.C. § 6103, the Health Insurance Probability and Accountability Act, the Children’s Online Privacy Protection Act, the Telephone Consumer Protection Act, the Electronic Communications Privacy Act, the Cable Communications Policy Act, the Video Privacy Protection Act, the Gramm-Leach Bliley (Financial Services Modernization Act), the Controlling the Assault of Non-Solicited Pornography and Marketing Act, and the Health Information Technology for Economic and Clinical Health Act); *Final Rule*, *supra* note 26 at 32,260-61 (same).

owners from the default-disclosure in unforeseen situations that require privacy.⁹³ For example, even though BARR as an opt-out system allows aircraft owners to submit a request that would take effect up to two months later, it does not protect individuals who become the victim of stalking with no notice, as with John and Martha King.⁹⁴ The Kings own a pilot-training school and became aware, after-the-fact, that someone had been tracking where their aircraft were located, and from that information, could tell when they were not at home.⁹⁵ Had BARR been an opt-in system prior to this occurrence, thereby requiring the Kings to give consent for the FAA to release their data, they would have had the opportunity to consider possible consequences of disclosure such as this type of stalking.

Whether businesses and corporations qualify as “individuals”⁹⁶ under the Privacy Act is not yet settled; however the law seems to be leaning towards the negative answer.⁹⁷ If a business does not qualify for “individual” status, it will therefore not qualify for Privacy Act protections, as only “individuals” are afforded protection.⁹⁸ In *Cell Associates v. National Institutes of Health*, the Ninth Circuit found that corporations do not have standing to sue under the Privacy

⁹³ The Privacy Act states that “[n]o agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, *except pursuant to a written request by, or with the prior written consent of, the individual* to whom the record pertains.” 5 U.S.C. § 552a(b) (emphasis added)

⁹⁴ See Comment to Access to Aircraft Situation Display (ASDI) and National Airspace System Status Information (NASSI), 76 Fed. Reg. 12,209 (proposed Mar. 4, 2011) (anonymous commenter, titled *Five Compelling Reasons Why Government Policy Should Not Trample Privacy and Security*); *BARR Program in Jeopardy*, NATIONAL BUSINESS AVIATION ASSOCIATION (Mar. 21, 2011), <http://www.nbaa.org/ops/security/barr/impact/king-schools.php>.

⁹⁵ *Id.*

⁹⁶ See 5 U.S.C. § 552a(a)(4) (defining “record” by using the term “individual”); 5 U.S.C. § 552a(a)(2) (defining “individual”).

⁹⁷ “[The] term [‘individual’] is used instead of the term ‘person’ throughout the bill in order to distinguish between the rights which are given to the citizen as an individual under this Act and the rights of proprietorship, businesses and corporations which are not intended to be covered by this Act.” *Stone v. Export-Import Bank of the United States*, 552 F.2d 132, 137 n.7 (5th Cir. 1977), cert. denied, 434 U.S. 1012 (1978) (quoting S. Rep. No. 1183, 93d Cong., 2d Sess. 79 (1974), *interpreting* 5 U.S.C. § 552a(a)(2)). See *OKC Corp. v. Williams*, 461 F. Supp. 540, 550 (N.D. Tex. 1978) (“An ‘individual’ is defined by the Act as a ‘citizen of the United States or an alien lawfully admitted for permanent residence.’ ‘This definition is intended to distinguish between the rights which are given citizens and individuals under this Act as opposed to the rights of proprietorships, businesses, and corporations which are not intended to be covered by the Act.’”), *quoting* Privacy Act Guidelines, OFFICE OF MANAGEMENT AND BUDGET, 40 Fed. Reg. 28,951 (July 9, 1975) (internal citation omitted).

⁹⁸ 5 U.S.C. § 552a(a)(2), (4).

Act.⁹⁹ The Supreme Court also recently found that corporations are not entitled to “personal privacy”;¹⁰⁰ however, that was held within the context of FOIA’s exemption 7,¹⁰¹ and is not directly applicable to the Privacy Act. On the contrary, the Supreme Court has also held that a corporation was entitled to constitutional protection similarly to a natural person.¹⁰² Ultimately, while the Privacy Act and any protection of flight data it provides may or may not apply to aircraft-owning businesses also, it at least should apply to private, natural-person owners whose aircraft are flown under IFR using flight plans.

B. The Fourth Amendment Provides a Standard for Privacy in the Civil Context

To make the argument that “concerns about warrantless surveillance are not relevant” to a disclosure of this nature, the FAA cited to *United States v. Knotts*,¹⁰³ a 1983 Supreme Court case discussing the use of electronic surveillance as a substitute for physical following.¹⁰⁴ In *Knotts*, the Court found, it permissible for the police to use a radio transmitter that, once affixed to the suspect’s vehicle, enabled the police to follow the vehicle.¹⁰⁵ The supporting reasoning relied upon by the FAA was that “[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.”¹⁰⁶

However, the high court also recently handed down a decision in another surveillance case, *United States v. Jones*,¹⁰⁷ this time discussing law enforcement’s use of a GPS device to

⁹⁹ 579 F.2d 1155 (9th Cir. 1978).

¹⁰⁰ Fed. Comm’n Comm’n v. AT&T, Inc. (*FCC v. AT&T*), 131 S. Ct. 1177, 1187 (2011).

¹⁰¹ *Id.*

¹⁰² *Citizens United v. Fed. Election Comm’n*, 130 S. Ct. 876, 899 (2010) (following extensive precedent that finds First Amendment protection to apply to speech regardless of whether it came from a corporation or a natural person).

¹⁰³ 460 U.S. 276 (1983).

¹⁰⁴ *Final Rule*, *supra* note 26 at 32263 n.2.

¹⁰⁵ The technology in *Knotts* consisted of a transmitter, attached to the suspect’s vehicle, and a receiver in the police vehicle. *Knotts*, 460 U.S. at 277, 282.

¹⁰⁶ *Knotts*, 460 U.S. at 281.

¹⁰⁷ 132 S. Ct. 945 (2012).

continually monitor a suspect's whereabouts.¹⁰⁸ In *Jones*, the Court affirmed the judgment of the D.C. Circuit in *United States v. Maynard*.¹⁰⁹ The facts of *Maynard* rested upon the use of GPS tracking as a substitute for physical police surveillance for twenty eight days.¹¹⁰ Writing for the court, Judge Ginsberg explained that an individual has a reasonable expectation of privacy in his movements over a period of time,¹¹¹ which is distinguishable from the lack of expected privacy in a more time-limited movement from one place to another.¹¹² In affirming the D.C. Circuit, however, the Supreme Court focused its analysis of the issue on the attachment and use of the GPS unit to the defendant's vehicle,¹¹³ which the Court found to be an unconstitutional search.¹¹⁴ In doing so, the Court expressly did not rule on the issue of whether continual electronic observation is constitutionally permissible.¹¹⁵ Even in affirming the Circuit court's judgment *Jones* did not overrule *Knotts*, because, as *Jones* notes,¹¹⁶ the *Knotts* Court expressly reserved the issue of whether continual surveillance for a case that actually brought the issue before the Court.¹¹⁷

Knotts was decided before advanced technology became so prevalent in our society, and the Court did not foresee the possibility of a case such as *Maynard*.¹¹⁸ Also, the holding in *Knotts* heavily rested on the fact that any member of the public, or a police officer, can easily follow a

¹⁰⁸ *Id.* at 948.

¹⁰⁹ 615 F.3d 544 (D.C. Cir. 2010).

¹¹⁰ *Maynard*, 615 F.3d at 555.

¹¹¹ *Id.* at 544.

¹¹² *Id.* at 558.

¹¹³ *Jones*, 132 S. Ct. at 948, 952.

¹¹⁴ The court noted how the government, through the police, had converted the use and functionality of Jones's vehicle through the attachment and use of the GPS transponder. *Jones*, 132 S. Ct. at 958.

¹¹⁵ *Id.* at 953-54 (“[O]ur cases suggest that such visual observation is constitutionally permissible. It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question.”).

¹¹⁶ *Id.* at 952 n.6.

¹¹⁷ *Knotts*, 460 U.S. at 284 (“If such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.”).

¹¹⁸ *Id.* at 283 (the “reality [of its holding] hardly suggests abuse”).

driver on public roads.¹¹⁹ However, this is not true in the case of an aircraft: it is extremely infeasible, if not completely impossible, to “follow” an aircraft, either in the air or on the ground, as it flies through public airspace.¹²⁰

Obviously, the privacy rights discussed in these cases are markedly factually distinguishable from the privacy interests in keeping aircraft flight information undisclosed. *Jones* was decided in a criminal context, where the government was trying to use the GPS-derived location data against him in court. The ASD location data is not gathered by or for law enforcement, and there is no argument against the government collecting the data as there is in a criminal context; rather, the issue is what the government does with the data after the collection. However, in both contexts the issue of GPS-derived data and the detailed accounting of an individual’s life that this type of data can reveal are present. Also, the Supreme Court has acknowledged on many occasions the fact that Fourth Amendment protections should also apply in a civil setting.¹²¹ In *Soldal v. Cook County*, the Court expressly reaffirmed the “basic understanding that the protection against unreasonable searches and seizures fully applies in the civil context.”¹²² Therefore, the level of protection given in the criminal context should serve as a standard for privacy in other settings with similar facts and interests, like with the ASD data.

Fourth Amendment protections and warrant requirements can be waived if the individual whose privacy is at issue consents to the government’s action.¹²³ When the government is relying

¹¹⁹ *Id.* at 281-82.

¹²⁰ Air Traffic Control does not provide directions and separation to an aircraft that doesn’t have a destination; the pilot of the aircraft has to request a clearance to a certain direction, which the Controller will do his best to comply with. *See generally* 14 C.F.R. §§ 91.1-91.219. Even if it were possible to listen to radio communications between the first pilot and Air Traffic Control to ascertain where he is headed, the second pilot would need to know about how far he expect to fly so he can have an appropriate amount of fuel on board.

¹²¹ *See Soldal v. Cook County*, 506 U.S. 56, 67 (1992).

¹²² *Id.* at 67 n.11.

¹²³ *United States v. Mendenhall*, 446 U.S. 544 (1980).

on an individual's consent as a waiver, the consent must be knowingly and voluntarily given.¹²⁴ In order to protect any unwarranted intrusion, a similar consent requirement should be built in to BARR. The present method of disclosing flight data unless otherwise requested serves as *implied* consent instead of affirmatively-given consent, which is contrary to the standard treatment of consent in a privacy context.¹²⁵ If aircraft owners had to submit a request to the FAA in order to have their movement information publicly disclosed, that would serve as their affirmative consent as is required by Fourth Amendment law.

C. Corporate Aircraft Owners Ultimately Receive No Help From FOIA's Exemption 4

Since corporate aircraft owners may not qualify for the same protections as individuals, either under the Privacy Act or the Fourth Amendment as discussed above,¹²⁶ it is appropriate to analyze protection they may receive elsewhere. The primary reason corporations have an interest in the privacy of their aircraft movements is to ensure competitors and other interested parties do not use that information to destroy their competitive advantage.¹²⁷ In fact, one commenter to the Proposed Rule, a corporation operating multiple brands of grocery stores in a variety of states, specifically noted that it uses BARR to keep “company and associate activities secure from competitive insight” while it “explore[s] areas for retail grocery development and travel to [] existing states of operation[.]”¹²⁸ Although the information filed in flight plans does not include the purpose of the flight or the entity being visited, it is often easy to deduce this merely based on the destination airport.¹²⁹ In fact, in an article and highly interactive website, the Wall Street Journal accomplishes exactly what this Note seeks to avoid: using the flight movement data

¹²⁴ *Id.*

¹²⁵ *Id.*

¹²⁶ See discussion of Privacy Act *supra* Part IIA.

¹²⁷ *Background of the BARR Program*, *supra* note 19; see also *Comments*, *supra* note 37.

¹²⁸ See Comment to Access to Aircraft Situation Display (ASDI) and National Airspace System Status Information (NASSI), 76 Fed. Reg. 12,209 (proposed Mar. 4, 2011) (comment of Delhaize America).

¹²⁹ See, e.g., Maremont & McGinty, *supra* note 86.

obtained from the FAA, it was able to combine information about the owner with the aircraft history to create a profile of where the owner has travelled and why he was visiting there.¹³⁰ An individual with this information regarding a corporate aircraft has the makings of a list of customers or suppliers of that company, which has already been found to constitute valid, protectable commercial information.¹³¹

FOIA exemption 4 excludes information from mandatory disclosure that consists of “trade secrets and commercial or financial information obtained from a person and privileged or confidential.”¹³² This analysis will focus on the second class of exempted information,¹³³ which includes material that meets the three prongs: 1) commercial or financial information; 2) obtained from a person; and 3) is privileged or confidential.¹³⁴ The D.C. Circuit has noted that “Congress contemplated that Exemption 4 ‘would include business sales statistics, inventories [and] customer lists.’”¹³⁵ Further, there is little debate among courts about whether customer lists are commercial information.

The analysis, then, focuses on the third prong; whether the customer lists at issue are privileged or confidential.¹³⁶ The standard for assessing confidentiality, as followed by a

¹³⁰ *Id.*; see also David Yermack, *Tailspotting: How Disclosure, Stock Prices And Volatility Change When CEOs Fly To Their Vacation Homes* (Nat’l Bureau of Econ. Research, Working Paper No. 17940, 2012) (comparing corporate jet flight information from the FAA with public real estate records to determine when CEOs and other officers were visiting vacation homes, and subsequently comparing that information with stock prices and corporate news disclosures).

¹³¹ *In re Uniservices*, 517 F.2d 492, 496 (7th Cir. 1975); Alan E. Littmann, Comment, *The Technology Split in Customer List Interpretation*, 69 U. CHI. L. REV. 1901, 1925 (2002).

¹³² 5 U.S.C. § 552(b)(4).

¹³³ Because the issue of whether customer lists qualify as trade secrets entails a largely factual analysis undertaken by the court on a case-by-case basis, this analysis will not focus on the possibility of companies’ customer lists qualifying for exemption 4 protection under the “trade secrets” class.

¹³⁴ *Getman v. Nat’l Labor Relations Bd.*, 450 F.2d 670, 673 (D.C. Cir. 1971). Some courts have separated “trade secrets” into their own class, effectively not requiring a showing of the same three prongs to be protected under exemption 4. *Id.*

¹³⁵ *Greenberg v. Food & Drug Admin.*, 775 F.2d 1169 (D.C. Cir. 1985), quoting H.R. Rep. No. 1497, 89th Cong., 2d Sess. 10 (emphasis added by the court).

¹³⁶ See *id.*; see also *United States v. Louderman*, 576 F.2d 1383, 1387 (9th Cir. 1978) (not upsetting the District Court’s jury instruction treating customer lists as commercial information by nothing that the lower court “instructed

majority of circuits,¹³⁷ is found in *National Parks v. Morton*. This standard provides that information should be treated as “confidential or privileged” for purposes of FOIA’s exemption 4 “if disclosure is likely to have either of the following effects: (1) to impair the Government’s ability to obtain necessary information in the future; *or* (2) to cause substantial harm to the competitive position of the person from whom the information was obtained.”¹³⁸ It is conceded that the government’s ability to continue to collect this information will not be impeded if BARR continues to operate as it does currently; the facts that filing the flight movement information is a prerequisite to flying in certain airspace, that the collection of flight information is necessary for safety reasons, and the lack of opposition to BARR in its current opt-out configuration shows the government’s continuing ability to collect the data. Therefore, the issue turns on whether the disclosure will cause substantial competitive harm to the disclosing companies.

To determine whether a disclosure will cause substantial competitive harm under this test, the Ninth Circuit stated that “the parties opposing disclosure need not show actual competitive harm. [] Rather, evidence revealing (1) actual competition; and (2) a likelihood of substantial competitive injury is sufficient to bring commercial information under Exemption

the jury regarding the term ‘property’ and stated that it encompasses ‘confidential and nonpublic commercial information such as customer lists’”).

¹³⁷ See generally *9 to 5 Org. for Women Office Workers v. Board of Governors of Fed. Reserve Sys.*, 721 F.2d 1 (1st Cir. 1983); *Nadler v. FDIC*, 92 F.3d 93 (2d Cir. 1996); *United Tech. Corp. v. Dep’t of Health & Human Servs.*, 574 F. Supp. 86 (D. Del. 1983); *Acumenics Research & Tech. v. United States Dep’t of Justice*, 843 F.2d 800 (4th Cir. 1988); *Calhoun v. Lyng*, 864 F.2d 34 (5th Cir. 1988); *GC Micro Corp. v. Def. Logistics Agency*, 33 F.3d 1109 (9th Cir. 1994); *Anderson v. Health & Human Servs.*, 907 F.2d 936 (10th Cir. 1990); *Hustead v. Norwood*, 529 F. Supp. 323 (S.D. Fla. 1981).

¹³⁸ *Nat’l Parks & Conservation Ass’n v. Morton*, 498 F.2d 765 (D.C. Cir. 1974) (emphasis added). The D.C. Circuit, followed by a District Court in the Eighth Circuit, has adopted a distinction between information provided voluntarily and involuntarily to the government, to be applied prior to reaching this test. *McDonnell Douglas Corp. v. NASA*, 895 F. Supp. 319, 325 (D.D.C. 1995). *McDonnell Douglas* noted the *National Parks* standard is applicable if the information has been provided involuntarily, and a separate test as stated in *Critical Mass Energy Project v. NRC*, 975 F.2d 871 (D.C. Cir. 1992), applies if provided voluntarily. *McDonnell Douglas*, 895 F. Supp. at 325. Because most jurisdictions ignore this distinction, and because filing the flight information via a flight plan is federally required in order to fly in certain airspace, this analysis focuses only on the relevant “involuntarily submitted” standard.

4.”¹³⁹ It would be simple for most corporations to make a showing of “actual” competition, even by just providing a list of competitors. Indeed, the Ninth Circuit brushed off the first prong and focused its discussion on the likelihood of substantial injury.¹⁴⁰ Typical destinations for a business jet include current and potential clients, vendors, suppliers, and any other type of partner, among others.¹⁴¹ Allowing third parties to track aircraft movements could substantially jeopardize a competitive advantage by providing an insight into current projects and clients.¹⁴² Therefore, it is likely that there is adequate reason to treat the flight movement information as confidential, and allow it to be exempted from FOIA.

In its Final Notice, the FAA expressly claimed that the movement information at issue is not considered “commercial” information under FOIA Exemption 4 and thus is not withheld.¹⁴³ To come to this conclusion, the FAA primarily relied on the reverse-FOIA case.¹⁴⁴ There, the court held the *list* of tail numbers currently utilizing the BARR program was not commercial in nature.¹⁴⁵ However, since it was not the issue before it, the court expressly declined to comment on whether Exemption 4 would apply if the actual movement data were included in the FOIA request.¹⁴⁶ Once this tracking and movement information is added to the issue, the analysis

¹³⁹ GC Micro Corp. v. Def. Logistics Agency, 33 F.3d 1109, 1113 (9th Cir. 1994) (*citing* Pub. Citizen Health Research Group v. FDA, 704 F.2d 1280, 1290-91 (D.C. Cir. 1983) and Sharyland Water Supply Corp. v. Block, 755 F.2d 397, 399 (5th Cir. 1985)); *see also* Gulf & W. Indus. v. United States, 615 F.2d 527 (D. C. Cir. 1980) (holding that it is not necessary to show actual competitive harm by release of the information to the public in order to qualify for the exemption. Actual competition and the likelihood of competitive harm are sufficient).

¹⁴⁰ *Id.* at 1114.

¹⁴¹ *Business Aircraft Uses*, NATIONAL BUSINESS AVIATION ASSOCIATION (2012), <http://www.nbaa.org/business-aviation/uses/>.

¹⁴² *Id.*

¹⁴³ *Final Rule*, *supra* note 26 at 32261.

¹⁴⁴ *Id.* The FAA also relies on another case; however the facts of that one are not relevant to this discussion.

¹⁴⁵ NBAA v. FAA, 686 F. Supp. 2d 80.

¹⁴⁶ *Id.*

would likely be different;¹⁴⁷ thus, this case cannot be relied on as support for the contention that the flight data is not commercial in nature.

As the FAA noted in its Final Rule,¹⁴⁸ the Supreme Court, in *Federal Communications Commission v. AT&T* (“*FCC v. AT&T*”), ruled that “personal privacy” as used in FOIA does not extend to corporations.¹⁴⁹ However, the issue in *FCC v. AT&T* revolved around an interpretation of exemption 7(c), which prohibits disclosure of information compiled for law enforcement purposes in order to protect personal privacy.¹⁵⁰ It is conceded that exemption 7(c) does not protect the disclosure of the movement data at the heart of BARR.¹⁵¹ In contrast, exemption 4 does not say that protecting “an unwarranted invasion of personal privacy” is an intended goal of the exemption.¹⁵² Rather, it aims to protect information “obtained from a person.”¹⁵³ The Supreme Court said in *FCC v. AT&T* that, as specified by Rules of Construction in the United States Code, the definition of “person” includes corporations.¹⁵⁴

Therefore, the movement data pertaining to corporate aircraft should be protected under FOIA’s Exemption 4. This means that the FAA would not be *required* to disclose the information under the Act; however, *CAN Financial v. Donovan*¹⁵⁵ has held that just because the government is not required to disclose information does not preclude the possibility that it is not permitted to do so.¹⁵⁶ In fact, the Seventh Circuit has held that, even though the agency has “no

¹⁴⁷ See Comment to Access to Aircraft Situation Display (ASDI) and National Airspace System Status Information (NASSI), 76 Fed. Reg. 12,209 (proposed Mar. 4, 2011) (comment of the National Business Aviation Association).

¹⁴⁸ *Final Rule*, *supra* note 26 at 32261.

¹⁴⁹ *FCC v. AT&T*, 131 S. Ct. at 1187.

¹⁵⁰ 5 U.S.C. § 552(b)(7)(C).

¹⁵¹ It is conceded that the movement data filed in flight plans is not primarily collected for “law enforcement purposes” as specified in exemption 7, which defeats any applicability even before reaching the issue of whether “personal privacy” should apply to corporations as discussed in *FCC v. AT&T*. While the information might sometimes be used in law enforcement, it is not the reason the information is collected.

¹⁵² 5 U.S.C. § 552(b)(4).

¹⁵³ *Id.*

¹⁵⁴ *FCC v. AT&T*, 131 S. Ct. at 1182-83 (citing 1 U.S.C.S. § 1).

¹⁵⁵ 830 F.2d 1132 (D.C. Cir. 1987).

¹⁵⁶ *Id.* at 1144.

commitment to withhold the document[,] if the balance inclines in favor of protection, [] maybe such a commitment is implicit.”¹⁵⁷

Even though the government cannot be required to maintain this information confidentially, it should still exercise its discretion to do so. A function of government is to protect the commercial interests of its industries. At the least, when deciding whether to release the movement information, the government should carefully balance the public benefit gained by release against the private commercial interests in keeping it private. In the present situation, there has been no showing by either the FAA or any other interested parties of a justifiable public interest in knowing where particular aircraft are at any given moment.¹⁵⁸

When discussing the merits of releasing the location data, a handful of commentors on the Proposed Rule mentioned a shareholder’s interest in monitoring his corporation’s use of business aviation;¹⁵⁹ however, concerns of this nature are not in the government’s interest and are best dealt with through disclosure methods internal to the corporation. Even a shareholder who could use the data to monitor his company’s aircraft would likely not want any potentially confidential information to be available publicly and to competitors, as that would also be harming his interests.

After all the relevant factors are weighted, there is ultimately no legal requirement, standard, or consequence for deciding either way. The FAA could reasonably decide that the current method of opting-in to BARR is sufficient to protect the concerns raised in the FOIA exemption 4 analysis;¹⁶⁰ if a company does feel like it needs competitive protection, it has the

¹⁵⁷ Gen. Elec. Co. v. United States Nuclear Regulatory Com., 750 F.2d 1394, 1398-99 (7th Cir. 1984).

¹⁵⁸ See *Comments*, *supra* note 37 (out of all 621 comments to the proposed rule, only 24 express any type of support for it, and of the few who supplied reasoning for the support, the main reason provided for the affirmative disclosure was curiosity about private jet usage.).

¹⁵⁹ *Id.*

¹⁶⁰ See discussion of FOIA’s exemption 4 *supra*.

option of requesting it and being automatically granted.¹⁶¹ The same possibility of unforeseeable or unexpected invasions of their “privacy” that exists with, and should be protected for, private citizens¹⁶² does not have an equivalent here, as corporations should be able to tell prior to using an aircraft if they have destinations to be kept confidential. Combining the lack of an affirmative privacy requirement for corporations with the fact that corporations have the ability to anticipate their need for privacy, the existing “opt-out” system may sufficiently protect any rights owed to corporate owners, and any change would likely be unnecessary for the protection of their interests.

D. Removing Tail Numbers as an Alternative to Changing BARR

If the FAA thinks it is too cumbersome to switch BARR from an opt-out system to an opt-in system, another option would be for it to remove the tail numbers from the data feed that is released to ASD subscribers such as FlightAware.com. An aircraft’s tail number, being equivalent to a vehicular license plate number, is the tag that connects the movement information to the individual owner.¹⁶³ Removing this identifier would allow private aircraft owners to retain their privacy, and would also allow the FAA to achieve its desired goal in originally introducing the Proposed Rule: greater government openness.¹⁶⁴ The practical result of this change would be that the public may still see where aircraft are located in the sky and how the (governmentally-run) air traffic controllers are handling them, but would not be able to tell who owns any particular aircraft.¹⁶⁵ Unfortunately, unless this system was also outfitted with an “opt-in” provision, it comes with a drawback: this alternative would remove the option of allowing an

¹⁶¹ See *Background of the BARR Program*, *supra* note 19.

¹⁶² See discussion of Privacy Act *supra* Part IIA.

¹⁶³ See *FAA Registry*, *supra* notes 69-70.

¹⁶⁴ See *Final Rule*, *supra* note 26 at 32,260-61; see also Open Government Memoranda and Directives *supra* note 43 (cited by the Proposed and Final Rules as justification for the attempted policy shift).

¹⁶⁵ It should be noted that this does not apply to aircraft operating commercially, as with the airlines. Even though these aircraft are privately-owned also, current protocol does not provide for the blocking of commercial flight data, nor should it. There is a valid public interest in being able to track the status of a commercial flight.

owner to allow his movement data to be released. For example, one of the comments in support of the Proposed Rule mentioned that as a pilot and aircraft owner, he liked to have his family be able to see where he was flying, both for entertainment and to allow them to know when he would be home.¹⁶⁶ This drawback, without the inclusion of an opt-in provision similar to the one discussed above, makes this option even less feasible.

CONCLUSION

Even though this issue is not widely addressed in the media and affects a very small percentage of the country, it is nonetheless very important to those who are affected. Currently, BARR protects only aircraft owners who affirmatively request to have their location and movement data withheld from public disclosure. Those who do not make this request are subject to automatic disclosure until such a request is made, plus a month or so for processing time. This system is likely in violation of prevailing federal privacy law with regards to natural-person aircraft owners because of its method of disclosing unless requested otherwise. The Privacy Act, at the forefront of federal privacy law, allows for disclosure if affirmative consent has been given by the individual about whom the record is maintained. BARR should be amended to reflect the “consent” aspect of privacy law and switch to a system of requesting that certain aircraft records be released instead of requesting that they be withheld. Since there is already a mechanism in place for requests to be submitted, this option is extremely feasible.

Although there has been a large shift toward an attitude of open government with the current administration, there is still substantial government and legal interests in protecting personal privacy rights. Having owners affirmatively give their consent to disclosure is essential in the modern reality of ever-expanding technology. If the FAA is still interested in following the spirit of the open-government initiatives by releasing the aircraft movement information, as it

¹⁶⁶ See *Comments, supra* note 37.

was when it published the Proposed Rule to amend BARR, it should consider removing the tail numbers from the data feed prior to granting public access to the ASDI system. Implementing this method would ultimately be the best way to balance individual privacy interests with the competing interest in government openness, the two factors whose balancing is really at the heart of all privacy and disclosure issues.