The Real First Class? Inferring Confidential Corporate Mergers and Government Relations from Air Traffic Communication

Martin Strohmeier*, Matthew Smith*, Vincent Lenders†, Ivan Martinovic*

*University of Oxford, UK †armasuisse, Switzerland

***Abstract*—This paper exploits publicly available aircraft meta data in conjunction with unfiltered air traffic communication gathered from a global collaborative sensor network to study the privacy impact of large-scale aircraft tracking on governments and public corporations.**

First, we use movement data of 542 verified aircraft used by 113 different governments to identify events and relationships in the real world. We develop a spatio-temporal clustering method which returns 47 public and 18 non-public meetings attended by dedicated government aircraft over the course of 18 months. Additionally, we illustrate the ease of analyzing the long-term behavior and relationships of aviation users through the example of foreign governments visiting Europe.

Secondly, we exploit the same types of data to predict potential merger and acquisition (M&A) activities by 36 corporations listed on the US and European stock markets. We identify seven M&A cases, in all of which the buyer has used corporate aircraft to visit the target prior to the official announcement, on average 61 days before.

Finally, we analyze five existing technical and non-technical mitigation options available to the individual stakeholders. We quantify their popularity and effectiveness, finding that despite their current widespread use, they are ineffective against the presented exploits. Consequently, we argue that regulatory and technical changes are required to be able to protect the privacy of non-commercial aviation users in the future.

1. Introduction

In recent years, the drive to modernize airspace has seen a push from international aviation organizations to use the surveillance technology Automatic Dependent Surveillance-Broadcast (ADS-B). Introduced to improve both the accuracy and efficiency—and thus safety—of airspace surveillance, this protocol indiscriminately transmits positional and identification information of aircraft on an unencrypted channel. In many parts of the world, it is mandated for usage on most aircraft in civil airspace by 2020 [37].

In this work, we explore a new affront to privacy in aviation and examine the effects of aircraft tracking by air traffic communication. Tracking movements of individual business, state or military aircraft can be impactful; recent examples include legal investigations into the Vice President of Equatorial Guinea exploiting intelligence gathered through ADS-B tracking [11] or revelations on the personal use of corporate aircraft by top management [18, 7].

To go beyond such anecdotes and provide a more complete picture, we analyze the impact that large-scale and long-term collection of aircraft communication data has on the privacy of aviation users. The difficulty of obtaining flight movement data has considerably decreased with the advent of affordable software-defined radios (SDRs), which make the reception of ADS-B messages (and thus the positional tracking of many aircraft) trivial. While installing a personal receiver can provide a range of up to 600 km, many fully-fledged commercial operations such as Flightradar24 [16] or FlightAware [15] pool air traffic control (ATC) data from such receivers and make it available online, adding a global dimension to the tracking of aircraft.

For the most part, the data on these services is largely publicly available and easily accessible. However, it generally excludes many types of aircraft considered sensitive, owned by stakeholders ranging from governments to corporations. In this work, we show that unfiltered ADS-B data, which is easily obtained from many sources, can impact the privacy of several of these aviation users when used in conjunction with publicly available aircraft meta data.

Concretely, we demonstrate that it can be used to identify co-location and meetings of such actors, from which it is feasible to infer confidential business knowledge such as the existence and timing of M&A negotiations. We further propose a spatio-temporal clustering approach, which identifies larger meet-ups of potentially 'interesting' aircraft and show that such an approach can reliably identify state/diplomatic meetings. Indeed, the exploitation of ATC data also sheds light on visits of governmental actors to foreign states and their relationships with other governments.

Naturally, not all of the concerned aviation users are happy with the public availability of and lobby for technical and legal restrictions on the tracking of their flights [27, 49]. We show that existing mitigation measures have remained ineffective thus far and new approaches are required to protect the privacy of non-commercial aviation users.

In this work, we make the following contributions:

- Using a real-world dataset spanning more than 200,000 aircraft over 18 months, we demonstrate concrete negative impacts on the privacy of two different user groups enabled through the

combination of modern ATC communication and aircraft meta data. For governments, we show that their derived movements provide insights into their meetings and relationships. For private corporations, we demonstrate the leakage of confidential business knowledge using the example of M&A negotiations.

- We analyze the effectiveness of all potential mitigation approaches available to individual stakeholders and provide quantitative data on how widespread these measures currently are. Based on this, we derive recommendations and guidelines for future regulations and technical developments.

The remainder of this work is organized as follows: Section 2 provides the necessary background to air traffic control and developments in wireless communications. Section 3 provides a perspective on the privacy of different aviation user groups. Section 4 describes our data collection setup and external data sources. Section 5 introduces the concrete analytic approaches that prove this impact. Section 6 provides our experimental setup and Section 7, the results. Section 8 analyses all available mitigation options. Section 9 discusses said results and Section 10 the related work. Finally, Section 11 concludes the paper.

2. Background

We provide a brief introduction to modern ATC and the wireless communication used to control the airspace.

2.1. Air Traffic Surveillance Technologies

Current ATC surveillance relies heavily on two technologies: ADS-B and Secondary Surveillance Radar (SSR). SSR is a cooperative technology comprising the so-called transponder Modes A, C, and S. Ground stations interrogate aircraft transponders in range using the 1030 MHz frequency and receive the requested information on 1090 MHz.

ADS-B is a more recent development: it is currently being rolled out in most airspaces and promises cheaper and more accurate surveillance [14]. In lieu of interrogations, the aircraft automatically fetches its own position via GPS and broadcasts it regularly and unencrypted (position along with velocity twice per second, identification every five seconds) to all other aircraft and ground stations in the vicinity. Figure 1 provides a high-level overview of both approaches.

A **24-bit address** assigned by the International Civil Aviation Organization (ICAO) to every aircraft (specified in [23]) is transmitted via both systems. Note, that this is different to an aircraft callsign or squawk. The callsign can be set through the flight deck for every flight, while squawks, of which only 4096 exist, are allocated locally by ATC. The ICAO identifier is globally unique, providing address space for 16 million assignments, and enables the continuous tracking of the movements of particular aircraft; while the transponder can be re-programmed by engineers, the identifier is not easily (or legally) changed by a pilot.

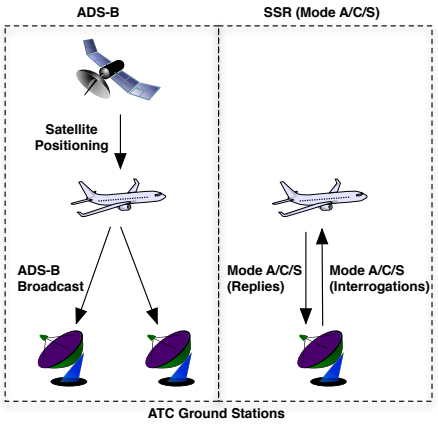

Figure 1. Overview of modern ATC technologies.

2.2. The Role of Software-Defined Radios

With SDRs becoming commodity technology, software is available for many types of radio frequency communication. An active community has made many modulation tools freely available and open source, lowering the bar to eavesdrop on and manipulate wireless communication. Examples include the easy access to mobile phone networks or satellite signals. As such, relying on protocol obscurity for security and privacy is no longer effective.

Aviation communication and flight tracking is one of the most active and popular SDR communities. Aviation enthusiasts can buy the popular RTL–SDR, a $10 USB stick re-purposed as software-defined radio receiver and use free software to receive practically all air traffic communication protocols in use today. Many planespotters around the world use SDRs to feed services such as Flightradar24 [16] or ADS-B Exchange [42], where global flight movements can be tracked live. Consequently, crowd-sourced data collected for flight trackers has been involved in flight incident investigations such as the two Malaysian aircraft lost over the Ukraine [20] and the Indian Ocean in 2014 [48], or the Germanwings crash [4]. This serves to illustrate the impact that the changing communications landscape has on the aviation industry.

3. Current State of Privacy in Aviation

In order to contextualize the issues presented in this paper, we first discuss the current state of privacy in aviation. We outline the threat model for aircraft tracking, the concerned stakeholders, provide a stance on the right to privacy, and highlight relevant legal and ethical challenges.

3.1. Threat Model

In our model, we define aircraft tracking as the act of obtaining live or delayed positional information on aircraft by purely passive actors. Their motivations range from traditional hobbyist planespotters, military and business interests, to criminal intent. Where traditionally most spotters had to

rely on visual means, i.e., seeing and recognizing the aircraft near an airport, SDRs have made accurate, fast and scalable tracking of transponder-equipped aircraft feasible.

For non-state actors, there are two options to exploit SDRs: using the data provided by commercial web services or installing their own ATC receivers. While a single receiver with a radius of up to 600 km can already provide interesting results, these are increased considerably with a larger network as considered by us. In principal, obtaining such large-scale data is feasible for any actor; live tracking data is available through public websites for continuous collection as is the required meta data (see Section 4).

3.2. Stakeholders

We briefly introduce the three different aviation user types that we consider in this work: the military, government and state aircraft, and business aviation.

3.2.1. Military Aircraft. Aircraft in use by the military use transponders to broadcast their altitude (Mode S) and/or position (ADS-B) as long as they operate in civil airspace. Safety requirements dictate that they cooperate with civil air traffic control and other aircraft sharing the skies. This makes it impossible for aircraft to 'go dark' and switch off all communications unless they are on a military mission. Consequently, military aircraft are trackable similar to all civil aircraft, apart from the fact that they can switch off their transponders when required.

3.2.2. Government and other State Aircraft. Despite the schedules of the most prolific members of government often being highly publicized, the exact routes and timings may need to be kept secret. Furthermore, air travel may be pertaining to sensitive diplomatic missions, which at the time of flight (or indeed at all) need to be kept out of public view. Similar concerns apply to other sensitive state aircraft operated by the executive branches, i.e., police, border control, or intelligence services. Whilst cooperation by tracking websites can make it harder to trace these aircraft, our results illustrate that it is easy to learn about their movements.

3.2.3. Business Aircraft. Many private users of non-scheduled aviation such as business jets seek to protect their business activities or do not like to broadcast their movements to the world in general. Business aviation groups have stated that the tracking of their members' aircraft can negatively impact competitiveness [26] and undermine the personal safety and security of its passengers [49].

3.3. Existing Cases of Tracking Exploitation

The analysis of aircraft movements reveals information about the owners, their relationships and the way in which they use their aircraft. The existing use cases and groups interested in such analysis have been wide and varied:

- **Investigative journalism:** Official flight data provided by the American Federal Aviation Administration (FAA) has been used by journalists of the Wall Street Journal to analyze the extent of the private usage of company aircraft by executives [28]. Using the destinations of company aircraft flights obtained through a Freedom of Information request, they inferred the frequency with which CEOs and board members visited for example their family, holiday homes or other holiday resorts.
- **OSINT:** Open source information has enjoyed popular application in many areas, including private and public intelligence services, which utilize it for purposes of open source intelligence (OSINT) [40]. Real or perceived mistakes made by military aircraft that do not switch off their transponders while operating in covert missions are regular topics in mainstream and aviation news [5]. Previous work has discussed the potential impact of the increased and simple availability of air traffic communication on the ability of governments to keep such military and diplomatic missions secret [45].
- **International relations:** The project 'Geneva Dictator Alert' run by two journalists automatically tracks visits of the governments of authoritarian states to the Geneva airport based on their ADS-B callsigns and position [47]. Data from this project has led to responses of judicial and political nature [11]. Beyond this, reports about government aircraft have proven politically sensitive in various cases [24].
- **Stock trading:** Aircraft movement information has been exploited for stock trading as the destinations of high-level executives can give away potential hints for merger talks or other stock-moving events [17]. As any information that is not widely available yet, investors can systematically exploit such knowledge to benefit at the stock markets. As stocks typically move significantly on the official announcement of M&A news [30], having early information gives investors an edge that can be used in profitable trading strategies.
  While paying airport employees for in-person observations can deliver such information, it increases operational risk, does not scale and can potentially be illegal. Obtaining stock-related aircraft data in an automated, immediate, scalable, and publicly available way is thus of great interest to many people.

3.4. Stakeholder Right to Movement Privacy

The unencrypted nature of avionic communications coupled with numerous public information sources on aircraft pose a clear challenge to any aircraft user who desires privacy. Yet, no clear stance on the right to privacy in aviation has been developed by researchers, aviation actors or governing bodies to date. In this section, we set out our view, broken down along the stakeholder groups.

The basis of our stance is the *personal* right to privacy. This is enshrined in human rights law across the world, e.g., Article 8 in the European Convention on Human Rights [9]. It states that "Everyone has the right to respect for his private and family life". Furthermore, personal data can be sensitive and thus is protected by relevant data protection legislation in many countries (e.g., in the EU [12]).

Business aircraft (or aircraft owned by individuals and used for business) rely on privacy in order to be commercially competitive and to ensure fairness. For example, many businesses use trade secrets or develop intellectual property, which, if made public, could cause a loss in value of the company. There is a further legal requirement to keep particular business actions private, to avoid falling foul of regulations on fraud and insider trading [52]. Whilst we acknowledge that business movements may need to be audited by relevant government agencies, we do not believe that legal business operations have any requirement to be public. As such, we adopt the stance that business aircraft have not only a requirement for but also a right to privacy.

State aircraft, whilst often desiring privacy, should not generally expect it. At least in democratic countries the electorate should be able to hold the government accountable, which requires an element of transparency. Whilst there are instances in which government transport might need to be kept private momentarily, most day-to-day government operations should not be secret in order to provide said accountability. For many meetings and events, government attendance is publicly declared thus rendering privacy approaches irrelevant. As an example, even previously closely guarded meetings such as the World Economic Forum in Davos now publish an incomplete list of attendees, which regularly includes top-level government representatives [54]. Thus, we believe that on the whole, whilst governments may have a requirement, they do not have a comprehensive right to keep all state aircraft movements secret.

Military aircraft are primarily accountable along the chain of command of their country. Since their critical missions are typically operated outside of the civil aviation sphere, we claim that they have no special right to privacy extending beyond other state aircraft within this. It has to be considered that military aircraft have exceptional technical abilities to protect their privacy. Namely, they can switch off transponders or use systems which are exclusive to military aircraft [10, 22]. As they have the ability to use restricted (and thus private) channels to conduct their operations, any privacy leakage as a result of using civil technologies is a case of weak operational security rather than a sign of a requirement for privacy similar to individuals or businesses.

Tying these three stakeholders together is the question of whether, by using aircraft as they currently are (i.e. with very little capability to offer privacy) a stakeholder is simply waiving their right to privacy. We do not consider this to be the case since the aviation communication technologies which cause privacy leakage generally do not offer systems to protect them; in the few cases where such systems exist, they lack proper deployment or verification [39]. As explored later in the paper, all existing mitigation options do not effectively solve the problem at hand.

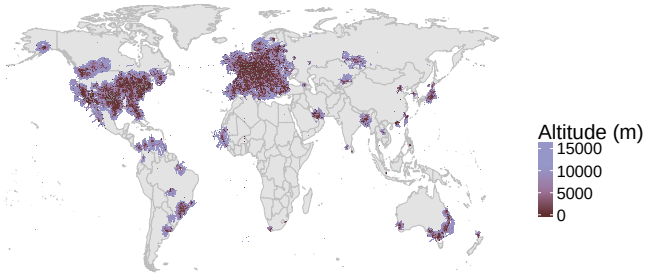

Figure 2. OpenSky coverage (June 2017). Darker colors indicate better low-altitude coverage.

3.5. Legal and Ethical Considerations

Since we were aware of the potentially sensitive nature of our research, we upheld strong ethical conduct throughout the work. While all data is publicly available in principle (it can be collected by anyone over time through installing receivers or using the live tracking APIs of several web services), we do not disseminate it ourselves in bundled and easily exploitable form. We do not mention specific individuals or business in this paper and ensured that all relevant laws and regulations were adhered to. Finally, we have notified the relevant government authorities and business aviation groups on submission of this paper.

However, as pointed out in the previous section, we believe that there is no trivially given right to privacy for all actors discussed in this work from an ethical standpoint. While private aircraft owners undoubtedly deserve privacy under normal legal circumstances, it is less clear for governments and authorities, who have to answer to their citizens and electorates. Regardless, all legal and ethical considerations are strongly overshadowed by today's technical reality as discussed in this paper. Consequently, Section 8 puts a spotlight on the futility of the currently existing approaches to prevent privacy leakages within civil aviation, in hope of real improvements for all aviation users in the future.

4. Data Collection

We require two separate sources of data, aircraft movement data based on ATC communication and aviation meta data collected from online sources.

4.1. The OpenSky Network: ATC Data

For our research we use live positional data provided by ATC protocols. Contrary to other means of obtaining flight movements, in particular freedom of information requests to aviation authorities (as used in [28]) this has the advantage of being immediate, globally applicable, uncensored and highly scalable. The OpenSky Network provides the data for our experimental studies collected via a participatory sensor

network.[1] It provides access to several years of raw messages as well as metadata through a fast query infrastructure, ideal for large-scale research projects. As of February 2018, it stores more than 5×10^{12} air traffic communication messages from six continents, captures daily more than 50,000 unique aircraft and has seen over 270,000 different aircraft overall. Fig. 2 illustrates the coverage at the time of writing with a focus on Europe and the US. All air traffic movement data used in this paper was collected by OpenSky's setup of readily- and cheaply-available commercial off-the-shelf receivers. OpenSky respects the operational security of aircraft operators and anonymizes the live public display of their identifiers on request. Consequently, researchers interested in such data for a specific academic purpose need to request assistance from the OpenSky Network association. For this study, we were able to obtain an unaltered dataset in order to conduct our analysis without restrictions. For more detail on OpenSky, its use cases and infrastructure see [37].

4.2. Aviation Meta Data Sources

In order to provide context to aircraft movements we use aviation meta data. Here, we discuss the availability and collection methods of the two sources required for a large-scale analysis: aircraft and airport meta data.

4.2.1. Aircraft Meta Data. There are several public data sources which provide meta-information on aircraft based on their identifiers: the aircraft registration or a unique 24-bit address provided by ICAO. This typically includes the aircraft type (e.g., Airbus A320) and the owner/operator (e.g., British Airways), which can be exploited for further in-depth analysis and stakeholder identification. We use several public database provided by third parties for our analysis of the aircraft meta data of ADS-B users, the main sources are described in the following:

- The first database is available and constantly updated in the Planeplotter software [6]. Our version of the database is from October 2016, containing 147,084 rows of aircraft data.
- The second database is available from Junzi Sun at TU Delft, comprising of a collection of all visible aircraft from a public flight tracker over a period of 18 months at the time of writing, amounting to 116,338 rows [46].
- The not-for-profit project Airframes.org is a valuable online source for general aircraft information offering comprehensive meta data about 747,126 aircraft. This includes background knowledge such as pictures and historical ownership information [25]. We use it as a first step to verify cases of uncertainty.
- For aircraft registered in the USA, the FAA provides a daily updated database of all owner records, online and for download. These naturally exclude any sensitive owner information but overall contain 320,777 records at the time of writing in March 2017 [13].
- Furthermore, the plane spotting community actively maintains many separate databases with spotted aircraft. They usually operate SSR receivers and enrich the received data with information such as operator, type, or registration manually. The database structure of Kinetic Avionic's BaseStation software has become the de facto standard format and is also used to exchange and share their databases in forums and discussion boards.

1. http://www.opensky-network.org

TABLE 1. DESCRIPTION OF OUR DATA SET CONTAINING METADATA OF 1,045,818 AIRCRAFT ICAO IDS.

Aircraft Affiliation	Aircraft	[%]
Business	97,372	9.3%
Military	519,235	49.6%
State-related	2,680	0.3%
Scheduled/General/Other	424,746	40.6%
Ground/Airport	1,785	0.2%

Table 1 breaks down the aircraft collected in our data set by their affiliation, which is determined primarily by the registrar. Where the operator is unknown, the type of aircraft (i.e., business jets, military aircraft) can give valuable insights for classification.

Note that these sources are naturally noisy, since they rely on compiling many separate smaller databases; aircraft around the world are registered, de-registered and transferred regularly. Thus, the aircraft identifiers used for the experiments in this paper were verified by hand using all available online information to ensure their accuracy.

4.2.2. Airport Meta Data. We require airport meta data to relate the concrete destinations of the tracked aircraft. We obtained the open airport database for our research from Openflights.org [32], which as of January 2017 contained 7,184 different airports around the globe, including name, ICAO and IATA (International Air Transport Association) short codes, and their precise location.

5. Large-scale Analysis of Aircraft Movements

We now describe several approaches that evaluate the privacy impact of exploiting large-scale and long-term aircraft movement data in combination with meta data on the types, owners, and operators of these aircraft.

First, we show that it is feasible to detect meetings of particular groups of entities that use unique, personalized aircraft. Second, we describe features based on the same data and how they can be used to analyze the movements, behavior and relationships of these entities. Finally, we describe a design intended to detect confidential events in the business world by predicting mergers and acquisitions.

5.1. Detection of Important International Events

The key insight to our first approach is the fact that a localized gathering of a certain amount of users of aircraft

Algorithm 1 Spatio-temporal clustering of aircraft. Requires $flights$, $decayTime$, $range$, $clusterSize$ as input. Outputs all clusters found into $interestingClusters$.

```
lastPositions, interestingClusters = [ ]

while !isEmpty(flights) do
    if lastPositions.contains(flight.operator) then
        lastPositions.remove(flight.operator)
    end if
    lastPositions.add(flight)
    for all flights do
        if currentTime > flight.time + decayTime
        then
            lastPositions.remove(flight)
        end if
    end for
    cluster ← findCluster(lastPositions, range)
    if cluster.size >= clusterSize then
        interestingClusters.add(cluster)
    end if
end while
```

of interest (AoI) is inherently noteworthy as a piece of intelligence. Regardless whether the targets are business, governmental or other types of aircraft, we develop an agnostic algorithm that is able to reliably detect such localized AoI gatherings live or with historical data.

Concretely, our goal is to find clusters of interesting aircraft which are simultaneously within a small area on the ground, i.e at the same airport or other airports very close by. For this to work, we require two things: the knowledge to classify particular aircraft as belonging to a group of interest and the ability to track these aircraft's movements, or at least their destinations.

Using this data, we develop an algorithm that sequentially takes the final position of the tracked AoIs and the timestamps associated with those positions and outputs all interesting clusters. Algorithm 1 describes our approach on a high level. Besides the input tracking data, it requires the parameters $decayTime$, $range$, and $clusterSize$. It then operates as follows:

- We assume a flight is completed and the aircraft has landed in the surrounding area of its last position report, if the last reported altitude of its approach is below 1000 m.[2]
- After each new completed AoI flight, the operator, its last position, and time stamp of this position are added to a database. If this aircraft or an aircraft by the same operator is already in the database, it is replaced with the newer data. Data older than $decayTime$ is removed to not distort the search algorithm, as it is assumed that the aircraft has left the area without being picked up by a receiver.
- Following any new flight addition, a geometric range search [1] for potential clusters is conducted, parametrized by the minimum number of aircraft $clusterSize$ that are within a given radius $range$.

The resulting output provides all clusters of AoI within the given parameters, including the participants of the meeting. From the weighted center of the cluster, we can infer the geographic location of the closest airport(s) in particular. This can then be used as a starting point for further analysis, such as connecting it to relevant news reports about meetings in the area. We will evaluate our algorithm using government aircraft in Section 7.1

5.2. Relationship Analysis

Beyond the detection of larger clusters, there are two separate features of interest that can be derived from aircraft movement data to describe the behavior of their users: destination airports/countries and the relationships with other aircraft operators. In combination with meta data, both features provide insights into the networks of an aircraft user be they private, commercial or diplomatic.

- **Airports/host countries:** The first key feature to analyze is the type and frequency of the destination cities, airports, and countries an aircraft is visiting. By matching the location of the last broadcasted position of each seen flight with the closest airport and city, it is possible to build longer-term movement profiles of all tracked aircraft. The frequency and timing of visits to a particular city can give insights into private or business habits [28]. Likewise, visiting specific countries in general can have impactful consequences for certain actors, if noticed by the public or journalists [11].
- **Aircraft relationships:** The second feature leaking private information on high-profile aviation users is found by comparing longer-term movement patterns of two aircraft. By exploiting their spatial and temporal relationships, i.e. analyzing when, where, and how often multiple aircraft reside at the same location at the same time, we can establish potential relationships between the owners, operators, or users. While coincidences in such a feature will be common and need to be taken into consideration, it can provide a starting point for further investigations. Naturally, stronger relationships are less likely to be chance or noise.

It should be noted that the features could also be obtained through listening to ATC voice communication, however our approach has the key advantage of worldwide scalability, with easy extraction and handling of relevant features. We extract these features for a case study of the behavior of government aircraft in Europe in Section 7.2.

2. As ADS-B transmissions are line-of-sight, only receivers in a very exposed position or located directly at the target airport are able to follow the transmissions fully to the ground. Taking the last known position below 1000 m, ensures that the vast majority of flights are useable for our purposes.

5.3. Predicting Mergers and Acquisitions

To illustrate the potential impact of non-existent aircraft privacy on businesses, we aim to show correlation between corporate flights and M&A transactions. We hypothesize that it is possible to analyze the movement information of the aircraft owned and operated by large businesses to infer potential negotiations related to M&A events.

We propose the following approach:

1) Identify the corporate aircraft of major companies using our data sources described in Section 4.2.
2) Identify all potentially interesting M&A events in relationship with these companies since July 2016. This includes the names and the location of the headquarters of the acquisition/merger target. Furthermore, it requires the date of the relevant, legally required, public announcements concerning the transaction.
3) Obtain the flight destinations of the corporate aircraft during the relevant time frame.
4) Identify the number of flights that happened in spatial and temporal proximity to the target HQ and the announcement of the transaction.

We predict that aircraft of a company looking to take over another company should be seen to land near the target's HQ prior to the merger announcement. The effect should be stronger compared to other, similar, companies' aircraft not involved in a relationship with the target. We test and evaluate our approach in Section 7.3.

Note, that this approach can naturally not establish causation, i.e., prove beyond doubt that flights to a target's HQ were directly related to these transactions. However, coupled with other available open source information, it can provide part of the picture for an investor and indeed all other interested market actors. We thus make the assumption that actors, which do everything to keep early negotiations and in particular the timing of important announcements secret, are not amenable to leaking their business-related movements. There may be many other ways to exploit the movements of business aircraft, however, we believe our approach provides a straightforward hypothesis to test and a strong proof-of-concept that privacy leakage in this domain exists.

6. Experimental Design

We now describe the experimental design used to evaluate the effects of aircraft tracking on the privacy of the different stakeholders. We detail the datasets that we use as inputs: the events we chose as ground truth to calibrate the clustering algorithm, and the groups of aircraft operators whose relationships and movement patterns we aggregated in 2016 and the first half of 2017.

6.1. Tracking Datasets

We constructed a hand-verified list of governmental and corporate AoIs to conduct our experiments. For all aircraft, we required their unique 24-bit ICAO identifier obtained through sources described in Section 4.2.

TABLE 2. DESCRIPTION OF THE GOVERNMENT DATASET. DATA COLLECTED WITH OVER 700 DIFFERENT SENSORS DURING 2016 AND THE FIRST HALF OF 2017.

Region	Gov AC	Tracked AC	Gov	Tracked Gov	Flights
Europe	170	135	33	33	12153
Americas	66	54	14	12	2489
Africa	113	52	33	24	520
Asia	64	43	18	15	680
Oceania	8	7	3	3	319
Mid. East	121	90	12	11	3142
Sum	542	381	113	98	19303

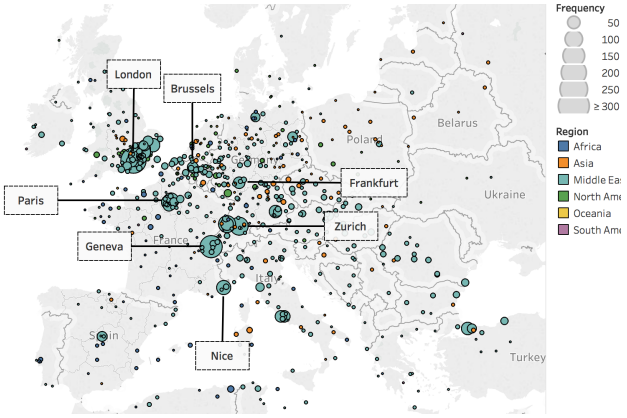

Figure 3. Non-European government aircraft visits at European airports during 2016/17. Colors indicate top origin region of the tracked aircraft.

6.1.1. Governments. Overall, this returned a list of 542 verified government AoI from 113 different states. Table 2 shows the distributions of these aircraft and their operating governments per World region.

To conduct our empirical evaluation, we obtained a full ATC communications dataset from the OpenSky Network, consisting of 19,303 flights with identifiable landings by aircraft on our governmental AoI list, seen between 1^{st} January 2016 and 30^{th} June 2017 (see Table 2). Of these, 15 states did not show up in the data, meaning their aircraft did not enter the coverage area during the collection time frame or they did not broadcast their position to our network using ADS-B. While a majority of the observed flights was unsurprisingly from the 33 tracked European states, we have seen 65 other governments from all corners of the World. Figure 3 illustrates the most popular government destinations within Europe per region of origin. The median number of completed flights per trackable government aircraft was 17.

6.1.2. Corporate Jets. We sampled 88 corporate jets that were clearly identifiable as registered to a major corporation listed on the major European or US stock market indexes. For these 88 jets, belonging to 36 different companies, we obtained their movements as seen by OpenSky, beginning

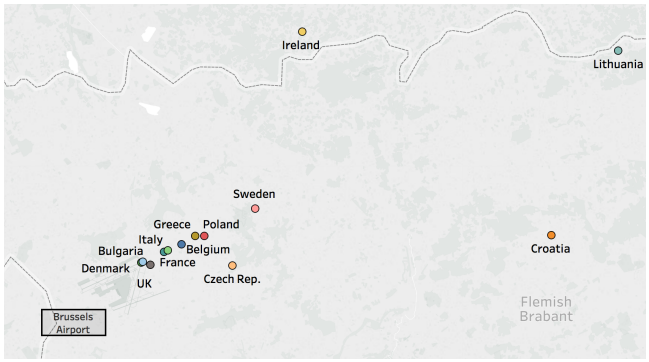

Figure 4. Government aircraft's last positions when landing at Brussels Airport for the EU Summit 20^{th} October 2016.

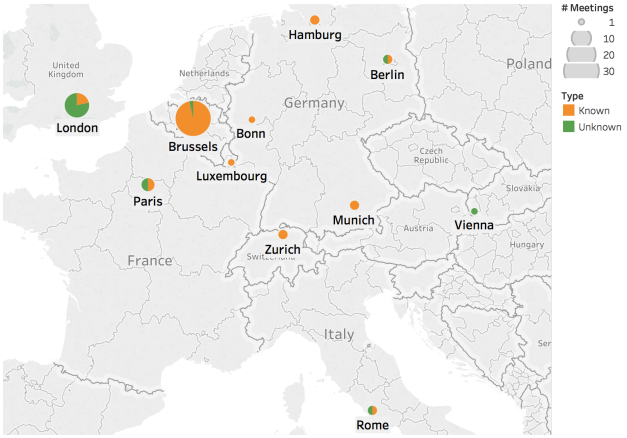

Figure 5. Distribution of government meetings across Europe 2016/17.

from 1^{st} January 2016 and ending 30^{th} June 2017. Overall, 75 of these aircraft were seen by OpenSky in the observed time frame, which provided us with a dataset that consisted of 12,008 flights with landings. The median number of completed flights per trackable corporate aircraft was 91.

6.2. Ground Truth Events

We obtained several ground truths for our evaluation. These are easily identifiable and widely publicized events that serve to show the effectiveness of our tracking approaches. To train the spatio-temporal clustering method, we used the well-known EU summits. To test the hypothesis that M&A transactions can be detected, we identified potential targets in our coverage area that we aimed to predict.

6.2.1. EU Summits. We used the European Union summits of the year 2016 as ground truth for the calibration of the spatio-temporal clustering. In general, any EU summit has a representative of all 28 governments attending, often via air travel, providing the basic case study for our hypothesis. EU summits are typically 2 days, with potentially related meetings often prepended. These summits all occurred in Brussels, Belgium on the following dates: $18^{th} - 19^{th}$ February, $17^{th} - 18^{th}$ March, $28^{th} - 29^{th}$ June, $20^{th} - 21^{st}$ October and $15^{th} - 16^{th}$ December.

6.2.2. M&A Transactions. For the previously collected 36 corporations, we identified their M&A activities as announced in the year from 1^{st} July 2016 to 30^{th} June 2017. We focused exclusively on acquisitions with European companies as targets because their headquarters are within the traditional core coverage area of OpenSky, providing a sufficiently high density even of low altitudes for all of the observed time frame. Overall, we identified 7 acquisitions of interest, conducted by 5 different corporations, that matched these criteria: in 3 cases, the buyer company was from the EU, in 4 cases from the US. For all cases, we collected their announcement date[3] and the position of the target's headquarters. We used the other 31 companies that did not have such transactions as a control group. In accordance with our stance on privacy discussed in Section 3.4, we anonymize all references to these private businesses. We note that the sample size is constrained by both the available tracking data (18 months, comprehensive coverage restricted to Europe) and the necessity to identify stock-listed company beyond reasonable doubt. Thus, it is infeasible to conduct a large-scale prediction analysis, but we believe our evaluation is sufficient to show the existence of privacy leakage.

3. Normally, this is the required official ad-hoc notification. In one case, the merger was leaked early, hence we used the date of the leak.

7. Evaluation

This section evaluates our approach. We first discuss the effectiveness and precision of our event detection algorithm. In the second part, we analyze the relationships and behavior of government aircraft in Europe before evaluating the M&A detection approach.

7.1. Detection of Government Events

We first tested whether the event detection algorithm detected all five ground truth events in Brussels in the year 2016 and calibrated the parameters $decayTime$, $blockTime$, $range$, and $clusterSize$ accordingly. Our results indicated that a $range$ of approx one degree (approx. 111 km) with a $clusterSize$ of 5 provides very reliable detection results with no noise in the given government meeting scenario. Figure 4 illustrates the process using one detected EU summit in Brussels on 20^{th} October 2016, showing 10 aircraft operated by EU governments landed at Brussels Airport and 3 further aircraft near Brussels where contact to the OpenSky receivers was lost.

Table 3 provides an overview of all detected events and the regions of the tracked participants based on the chosen settings. For the five EU summits used for training, we saw 18 out of the 19 EU governments with official aircraft for which metadata was obtained, missing only Portugal. This shows the effectiveness of the data collection and the clustering approach. We assume the remaining 10 governments did either not broadcast their aircraft positions or used other means of transport (air or ground) for these meetings.

TABLE 3. REGION-GROUPED STATE AICRAFT ATTENDING ALL DETECTED EVENTS WITHIN THE OPENSKY NETWORK COVERAGE. MINIMUM CLUSTER SIZE OF 5 AND 1° RADIUS AS OBTAINED FROM THE EU SUMMITS (2016) TRAINING DATA.

Event Type	Events	Location(s)	Avg. # of Participants	Participants by Region (Cumulative)						
				EUR	AME	AFR	OCE	ME	Asia	Sum
EU Summits (2016)	5	Brussels	11	20	0	0	0	2	0	22
EU Summits (2017)	4	Brussels, Rome	8	15	0	0	0	0	0	15
Foreign Affairs Council	7	Brussels, Luxembourg	6.1	13	1	2	0	2	0	18
Eurogroup Meetings	4	Brussels	6.3	11	1	0	0	2	1	15
Other EU Meetings	5	Brussels	5.8	11	1	0	0	2	1	15
World Economic Forum	2	Davos	17	8	2	5	0	6	3	24
Munich Security Council	2	Munich	11	6	1	1	0	5	3	16
G20 Meetings	3	Berlin, Hamburg, Bonn	9	6	2	5	0	3	0	16
NATO Meetings	2	Brussels, Rome	9.5	11	2	0	0	1	0	14
Anti-Corruption Summits	2	Paris, London	7	5	1	2	0	4	0	12
Global Peace Conferences	7	Brussels, Washington, London, Paris	8.4	13	4	3	1	8	3	32
Other Summits	3	Washington, Jakarta, Hamburg	10	10	2	4	1	6	4	27

Besides these summits provided by our ground truth, the algorithm picked up 41 further clusters in the observed 18 month period which we could relate to newsworthy high-profile gatherings of governments. We have aggregated these events into 11 groups, according to their purpose. Four of these are other meetings of European institutions, mostly in Brussels and Luxembourg. The other 7 comprise several different types of major global conferences from the World Economic Forum (WEF) in Davos (detected twice), over the Munich Security Council and NATO Meetings to Global Peace and Anti-Corruption summits.

Table 3 lists the number and origin of the participants. While it is not surprising that European governments dominate the conferences held in Europe, global conferences such as the Nuclear Summit in Washington and the 2017 Indian-Ocean Rim Association (IORA) meeting in Jakarta show a more diverse visitor profile. While for many meetings the list of attendees is known, some are incomplete; for both WEF instances we found several participating governments that were missing from the officially published lists [54].

Finally, the algorithm picked up government gatherings in 5 different European cities that were unrelated to a newsworthy summit-type event. Of these, the majority were in London, with others in Paris, Rome, Brussels, and Berlin (see Figure 5). We can speculate that these may be low-key multilateral meetings, several bilateral meetings in parallel by coincidence, or, as the vast majority of these events concerns London, the tending to local, potentially private, matters in the city by the mostly Middle Eastern participants.

Overall, we can conclude that the algorithm successfully picked up all ground truth events, and added further high-profile events in our coverage range. Naturally, there will be a trade-off depending on the parameter settings: with smaller $range$ and larger $clusterSize$, the chance to miss important events increases, while for smaller $clusterSize$ below 5 and $ranges$ greatly in excess of 100 km, false positives or noise becomes more likely.

TABLE 4. TOP EUROPEAN DESTINATIONS OF NON-EUROPEAN GOVERNMENT AIRCRAFT FROM JAN. 2016 TO JUNE 2017 (20+ VISITS).

State	Country Visited	# Visits
Dubai	United Kingdom	237
Qatar	United Kingdom	171
Bahrain	United Kingdom	102
Saudi Arabia	France	65
USA	Germany	52
Jordan	United Kingdom	50
UAE	United Kingdom	45
Morocco	France	38
Abu Dhabi	United Kingdom	37
Azerbaijan	United Kingdom	36
Turkey	Germany	34
Kuwait	Switzerland	29
Oman	Germany	28
Turkmenistan	Germany	23
Ivory Coast	France	21

7.2. Relationships between State Governments

Next, we evaluate the extended possibilities of government aircraft tracking by analyzing the relationships and movements of state governments in Europe over 18 months from the beginning of 2016. Table 4 shows the most popular airports and destination countries for the top non-European visitors in our European coverage area. We can see that the UK is by far the most popular single destination for such governmental visitors from other countries, featuring 7 times in the top 15 governments. This is followed by Germany with 4 occurrences, France with 3, and Switzerland with 1. The most frequent observed visitors to Europe hail from several Gulf States, but also North Africa and the USA.

Whereas in some countries the distinction between official and non-official use of state-owned aircraft may be blurred, diplomatic visits of all kinds are regularly part of high-profile political debates [41]. Consequently, concrete

TABLE 5. RELATIONSHIPS BETWEEN SELECTED GOVERNMENTS AS REFLECTED BY NUMBER OF POTENTIAL MEETINGS IN EUROPE DURING THE YEARS 2016/7. GOVERNMENTS SELECTED BASED ON THE HIGHEST FREQUENCY OF MEETINGS.

	Qatari	US	Swiss	Saudi	Netherlands	Swedish	Turkish	Slovakian
German	38	109	49	17	100	63	49	35
French	79	9	28	104	24	8	15	11
Belgian	15	27	9	7	93	47	29	28
Dubai	86	13	34	30	5	—	13	8

TABLE 6. CORPORATE AIRCRAFT VISITS (LANDING WITHIN 100 KM) AT THEIR TAKE-OVER TARGET LOCATIONS DURING DIFFERENT TIME PERIODS.

Absolute visits	**Monthly AVG 12-2 mon. before**	**Monthly AVG 2 months before**	**Month before**	**Month after**	**Monthly AVG 6 months after**	**Last seen before announcement [Days]**	**Combined share price change [%]**
Case 1 (EU/EU)	0.11	1	0	2	0.67	50	6.71
Case 2 (EU/EU)	2.56	2.5	2	0	0.75	25	1.1
Case 3 (EU/EU)	0	1	2	4	1.56	20	1.96
Case 4 (US/EU)	0	2.5	3	0	0	8	1.83
Case 5 (US/EU)	0.11	0	0	0	0	325	0.2
Case 6 (US/EEA)	0.22	6	12	2	5	1	20.29
Case 7 (US/EU)	0.29	1	2	0	1	1	23.18
Average	0.47	2	3	1.14	1.28	61.43	7.9
Control group	0.14	0.33	0.40	0.42	0.34	-	-

data such as those provided by government aircraft may often be able to aid in journalistic investigations and to evaluate claims made by the involved actors. Naturally, analyzing the reasons and motivations for specific relationships and government movements is out of the scope of this paper.

Similarly, Table 5 shows the top relationships between all government aircraft in Europe during 2016/7. The top three relationships have seen two governments at the same airport for 109 times (Germany/US), 104 times (France/Saudi Arabia), and 100 times (Germany/Netherlands), respectively. Whilst there is the possibility that government aircraft are in the same location at the same time, this becomes much less likely for the consistently high numbers of meetings we have seen over a prolonged time frame for many government pairs. Overall, we detected 7291 meetings over 1097 different relationships (median = 3).

7.3. Predicting Mergers and Acquisitions

Table 6 provides the numeric results of our approach to predict mergers. For each merger case, we have split the analyzed time frame into months before the merger and months after the merger. We provide the values for the month before and the month after, the average of the two months before, the monthly average of the year before (excluding the 2 months prior), and the monthly average until up to 6 months after the merger.

Of the 7 identified M&A cases in our dataset, all 7 takeover targets have been visited by aircraft owned or operated by the buying company in the year before the merger announcement; on average the last time they visited was 61 days prior. Concretely, 5 out of 7 have landed in the vicinity of the target HQ in the month prior to the announcement, between 2 and 12 times. The average of 3 visits is significantly different to the average of 0.4 found in the control group of 31 non-related US/EU stock-listed corporations with exclusive jets for management travel.

While false positives are always possible, in particular with large datasets, this shows that ATC data can provide an additional signal for stock market investors and other interested market participants. By also accounting for the basic viability of potential buyers (e.g., industry, relative size of the companies), false positives can further be minimized but we consider this out of scope for this paper.

We can see similarly significant results if we extend the period to 2 months. During this time frame, 6 out of 7 targets have been visited by their respective buyers, on average 2 times per month (compared to 0.33 by the control group companies). As expected, the effect tapers off after the merger announcement, even thought the companies are still more likely to be visited by the top management of their new owners: 3 out of 7 visited in the month after, and 5 did in the 6 months time period following the merger. The averages of 1.14 and 1.28 are still three times the averages of the control group (0.42 and 0.34, respectively).

The smallest difference can be found in the period between 2 and 12 months before the announcement. While 5 out of 7 companies flew to their targets HQ in during these time, the average was only 0.47 visits/month.

Overall, the evaluation shows that buyers of stock-listed companies with corporate aircraft indeed use them to fly to the corporate HQs of potential merger targets before the official announcement. Secondly, the most likely period to visit is 1-2 months prior to the announcement; in two cases even on the day before. As Table 6 shows, the mean combined share price change of all involved listed companies on the day of the announcement was 7.9% across all 7 cases. Taken together, these results prove that there is a serious privacy leakage for corporations with corporate jets with the real potential of a direct impact on their businesses.

8. Analysis of Mitigation Options

After showing the impact of large-scale aircraft tracking on the privacy of both governments and businesses, we now discuss the available mitigation options and analyze their popularity and effectiveness. Concretely, we examine five different options: the blocking of aircraft displays by tracking websites, switching ADS-B transponders off, the use of pseudonymous identifiers, obscuring the owners and operators in public registries, and the use of commercial air transport services. Table 7 summarizes our results, which are based on random samples of 500 aircraft for the different stakeholders. For this we used the full government data set.

8.1. Technical Measures

First, we look at some technical measures available to stakeholders today, i.e., those that involve modifying the operation of avionics or the protocols for systems. These approaches provide some level of certainty in the effect they have when compared to non-technical measures, but at the expense of usually being more costly or difficult to implement. We do not consider potential future developments of new protocols as they are generally thought to require 15-20 years until deployment [45].

8.1.1. Switching off Position Broadcasts. One obvious mitigation option for aircraft operators is to not broadcast their precise position. As long as ADS-B is not mandated for every participant in civil airspace (i.e., until 2020), there are many operators who choose to delay the upgrade in the first place for reasons of cost, convenience, or indeed privacy [38]. Around 30% of all aircraft in our sample did not yet support ADS-B, which is in line with previous research [37]. On top of this, some operators, presumably those with state privileges and acting in accordance with ATC, can actively switch their ADS-B transponders on or off in-flight.

Popularity. We found some evidence of switched-off ADS-B transponders. For our sample of military aircraft, 8.6% used this approach in the observed civil airspace while 1.9% of the government aircraft tracked relied on this measure. For business aircraft, only 0.4% of those equipped with ADS-B switched their transponders off on occasion, either for full flights or parts of it. It has to be noted that this could also happen due to a transponder malfunction.

Effectiveness. However, switching off one's position broadcasts, deliberate or not, and regardless of whether it will continue in significant numbers past the ADS-B equipage deadline, is ineffective as a defense against any curious sensor network operator. As long as messages are sent via any wireless technology along with the aircraft's unique ICAO number, it is feasible to track said aircraft using several physical-layer localization options, including multilateration [36] and grid-based localization [43]. Both require several receivers in the target area but have been shown to be effective and sufficiently precise with the cheap off-the-shelf sensors used to acquire the data in this paper.

Even when multiple receivers are unavailable, ATC altitude messages give away the aircraft landing process and reduces the potential target airports to a few candidates.

Naturally, it is hard to localize aircraft that go dark and switch off most or all air-to-ground communication. For example, US Presidential aircraft Air Force One uses this capability. But this possibility is provided exclusively to military-operated aircraft with missions of the highest importance; switching off all transponders causes great disturbance to the affected airspace, since the safety of all airspace users is greatly affected (ATC will need to effectively clear the airspace around such a mission). On top of this, switching off ADS-B in a known capable aircraft might draw additional attention to the aircraft and its mission, which runs contrary to the original intention. Therefore, we rate the overall effectiveness of switching off ADS-B as *medium*; in practice it only deters actors with very limited abilities and will not be allowed from 2020 when the ADS-B mandate is fully implemented in US/EU airspaces.

8.1.2. Pseudonymous Identifiers. ADS-B can be served over the Universal Access Transceiver (UAT) data link as well, which offers a built-in privacy mechanism generating a non-conflicting, random, temporary identifier to avoid third-party tracking [29]. However, practical restrictions on flight conditions limit its usefulness especially against the scale of observation used in this paper.

Popularity. As we tracked all aircraft using the main ADS-B data link rather than UAT, none of the aircraft in our dataset have made use of pseudonymous identifiers. Indeed, UAT is only available to a limited subset of general aviation aircraft in the United States using non-Class A airspace (below 18,000 ft) with no current plans of further expansion. As such, this method is not available to the types of stakeholders considered in this paper.

Effectiveness. Furthermore, it has been shown that the identifier generated by UAT can be de-anonymized [35]. Thus, new protocols, which either properly implement pseudonyms or fully confidential transmission of sensitive data, need to be developed. This would defeat the tracking of particular aircraft and all privacy-impacting mechanisms relying on the continuity of ICAO identifiers. Yet, this would also require a long time to deploy widely and may not be desired by regulators, who are on record saying that they prefer open systems [10]. Finally, it has been shown that it is possible to fingerprint ADS-B transponders on the physical and link layer levels, which, in sufficient granularity, would circumvent even properly implemented pseudonyms [44].

8.2. Non-technical Measures

As an alternative to technical measures exist a number of other approaches ,which rely on human factors or regulatory measures to protect privacy. These particular approaches are much easier to implement than changing avionics but can come at the cost of only being a partial solution.

TABLE 7. ANALYSIS OF AVAILABLE TECHNICAL AND NON-TECHNICAL OPTIONS TO MITIGATE THE PRIVACY IMPACT OF AIRCRAFT TRACKING, DEPENDING ON DIFFERENT STAKEHOLDERS (PERCENTAGES CALCULATED USING A RANDOM SAMPLE OF 500 FOR ALL CATEGORIES).

	Mitigation Options	Block List	Turn off ADS-B	Pseudonyms	Obscured Ownership	Commercial Transport
Popularity	Military	86.7%	8.6%	None	Generally non-public	Low / Unfit
	State-related	36.6%	None	None	15.6%	Low / Unfit
	Government	66.2%	1.9%	None	40.4%	<41.5%[4]
	Business	56.0%	0.4%	None	68.6%	>53.3%[5]
Effectiveness		Low	Medium	Medium	Medium	High

8.2.1. Blocking Lists. Web services for aircraft tracking have been publicly available for more than 10 years. They attract considerable interest from plane-spotters and are met with suspicion by business aviation associations [26].

One approach to limiting the privacy impact of such trackers is through block lists. The most extensive of these is the FAA's Aircraft Situation Display to Industry (ASDI) program [31]. ASDI provides a feed of aircraft currently observed by the FAA, which is used as one source by flight tracking websites. Non-commercial aircraft owners can request for information relating to their aircraft be blocked from the feed—essentially stopping the public dissemination of data about their aircraft from this feed. In recent years, websites such as Flightradar24 have taken this further, complying with these block lists even for data obtained from other sources [53].

Popularity. To find out about the extent of display blocking by large web trackers, we analyzed our sample of aircraft equipped with ADS-B as seen by OpenSky and tested whether their flight history was available on popular flight trackers. Table 7 shows the break down of the popularity of block lists per stakeholder group.

We can see that the vast majority (86.7%) of the ADS-B equipped military aircraft seen by OpenSky are blocked. For the 542 government aircraft from our dataset, in the majority of cases, their flights are not displayed by the tracking website. Still, 183 or about one third of these government aircraft are visible on commercial trackers at the time of writing, indicating a lack of awareness about the problem. A further 18 aircraft had become blocked from display during the observation time frame (or went inactive).

Lastly, more than half of all tracked business aircraft (56.0%) are being filtered, making up a large part of all blocked aircraft due to their greater prevalence.

Effectiveness. Clearly, aircraft owners making a specific request to limit public display of their movements have a proven interest in privacy. However, given the ease of installing an ADS-B sensor for anyone, we argue that block lists are of limited value. On top of this, while many commercial tracking websites comply, other crowd-sourced services exist without any block lists such as ADS-B Exchange [42]. In this particular case, the website even actively identifies military or government aircraft to the public.

We would further argue that the fact that an aircraft is on a block list makes it interesting for plane-spotters of all motivations. Thus, this approach may even have an adverse effect as it provides an additional signal. For example, when a new unknown plane is spotted and it is blocked, the interest in finding out more about the owner is automatically increased. Thus, we consider the effectiveness of this mitigation measure *low*.

8.2.2. Obscuring Ownership. Similarly to the blocking of flight data, some stakeholders use third-party entities to register their aircraft and conceal the real owner from public records. Popular methods include the use of shell companies (often offshore), special aircraft registration services, wealth management companies and trusts.

Popularity. Across all stakeholders in the US, we found over 12,000 aircraft registered by trusts and specialized services in the FAA records, accounting for over 3.75% of all aircraft registrations. Another 53,000 or 16.5% are registered to Limited Liability Companies (LLC), many of which follow the naming scheme NXXXXX LLC, where the so-called N number is the registration of the aircraft.

When breaking this mitigation option down by stakeholder, we can see stark differences in popularity. Among business jets, over 68% (see Table 7) use obvious obfuscation tactics in public aircraft registers, while only around 40% of government aircraft operators are actively obscured, with some aircraft registered in different countries, typically in recognized offshore financial centers (e.g., Bahamas or the Cayman Islands). This may reflect the greater accountability concerns governments have in many countries, compared to private businesses. Information about military aircraft is in general not available in any public register due to the very nature of their function. Furthermore, it has to be noted that not all countries around the world choose to publish their aircraft registration data because of general data protection concerns.

Effectiveness. Whereas this practice can mitigate some of the privacy problems created by public registries, it requires an almost impossible standard of operational security as a single slip up (e.g., being seen on the runway, or making connections between the shell company and the real owner in other registries) often means that their real users can eternally be obtained by a quick Internet search. While the gathering of such information provided on planespotting websites, social media, or aviation forums is tougher to automate, it is no hindrance to a determined attacker. Thus, the real-world effectiveness of obscuring ownership is *medium*.

4. Estimate based on 80 governments missing from our dataset.
5. Estimate based on data from German DAX30 companies [33].

8.2.3. Use of Commercial Air Transport. The most straightforward and effective approach to avoid the described type of privacy concerns is provided by not using designated aircraft, regardless of whether they are operated by the government, military or privately, and instead rely on more anonymous, non-exclusive transport means.

Popularity. Many of the governments missing from our dataset use commercial air transport for their travel: either they charter an ordinary jet, often from the country's flag carrier or private charter services, or they fly on scheduled airline services. The first option is popular for political or economical reasons [50]. As an example of the latter, the New Zealand government does not typically travel on designated aircraft; instead, members generally use commercial airlines [3].

Our dataset provides an upper limit for the popularity of this approach: Out of 193 countries currently in the UN [51], at least 113 use dedicated aircraft for government use, leaving at most 41.5% which exclusively use external options. Similarly, an analysis of the stock market index DAX, comprising Germany's 30 largest publicly traded companies, suggests that about half (53.3%) forgo corporate aircraft in favour of other options. This amount is likely to be higher for smaller companies. Lastly, the requirements for military or state aircraft (e.g., police, border or coast guard services) typically make the use of non-dedicated aircraft impossible for the vast majority of missions.

Effectiveness. As long as the callsigns of the perused aircraft remain inconspicuous, this is an effective defense that cannot be circumvented by exploiting air traffic communications. While mining news stories, social media, and aviation enthusiast websites may again be able to unearth some connections, this is out of the scope of our approach and generally harder to automate at scale with sufficient reliability. Contrary to the previous approach, a single slip up in operational security does not negate the actor's privacy in the past or future. Consequently, we class the effectiveness of this particular mitigation option as *high*, notwithstanding the fact that it is not a feasible option for many stakeholders. Nevertheless, we believe privacy may play an increased role in any future cost-benefit analyses concerned with owning aircraft versus chartering them.

9. Discussion

So far, we have demonstrated that tracking aircraft using core ATC systems allows us to learn much more than where an aircraft is. Correlation of first- and third-party data sources can reveal 'private' and confidential actions by businesses and governments alike. Importantly, this is with only a low level of investment in equipment and effort.

Even though options exist to mitigate the problem, they are largely ineffective against a reasonably powerful attacker and do not address the core issue that some stakeholder groups should be able to act in a private way whilst travelling via aircraft. This is most significant for business users who may rely on this to conduct business effectively.

Naturally, this work generates some recommendations for how to improve the state of privacy in aviation. In the short term, regulation provides a possible key to allowing relevant actors to protect their privacy. Governments would have to legally restrict and regulate those entities (private and commercial) that are sharing data about aircraft movements for which a reasonable effort at privacy has been made. This would need to be a more concerted effort than the ASDI scheme which is, to some extent, opt-in.

In the longer term, technical solutions should be developed to provide privacy guarantees; a robust pseudonym system could limit the tracking of aircraft over time. There is no critical technical or procedural need to have a consistent, publicly known identifier for aircraft—there is even evidence of aircraft being prescribed alternative IDs by the authorities in situations such as sensitive military flights [10]. Doing away with the inflexible current system in favor of a more transient one would in turn decorrelate consecutive flights by a given aircraft. This measure alone would greatly reduce the impact of ATC-based flight tracking.

Hence, in our opinion, the only way to effectively create the opportunity for privacy in ATC systems is through the combination of technical and regulatory measures. Regulatory measures can cover the case of data generated by state entities, but technical measures are needed to stop passive observers from easily collecting significant amounts of data.

As discussed in [45], there has been a preference for open systems in aviation, to increase safety through enabling maximum global compatibility. Naturally, this presents a conflict with the desire for privacy and security. Parallels can be drawn to the creation of the internet in that initially, open systems allowed easy integration and global interaction between different networks. However, in the longer term, malicious parties have resulted in both a desire and need for in securing all communications. Aviation networks carry bigger safety risk, so should aim for similar, if not greater, levels of security than the internet currently uses.

10. Related Work

Whilst the security implications of unencrypted ATC technologies have been widely discussed in the related work (e.g., [8]), and very recently efforts have been made to formally verify some avionics security protocols [2], the privacy impact has only been touched upon.

Regarding technologies which can be exploited to attack the location privacy of aircraft, Hoffman & Rezchikov presented a system which listens to ATC tower radio communications and uses voice recognition to extract ATC commands, through which they identify the whereabouts of blocked aircraft [21]. Specifically, this intended to erode privacy by creating a list of such blocked aircraft [19].

In the academic community, [34] discusses the issue of tracking aircraft using the ICAO in ADS-B messages. In the work closest to ours, the authors use historical flight tracks of US corporate aircraft released by authorities to show a relationship between CEOs' holiday schedules and their companies' news announcements [55].

Other technologies also can lead to privacy issues; in [39], the usage of ACARS by private aircraft is shown to reveal information such as aircraft intention and status, despite attempts to broadcast them confidentially. To the best of our knowledge, however, this is the first study on the real-world impact on aviation privacy caused by aircraft tracking.

11. Conclusion

In this paper, we have explored the privacy impact of combining easily available air traffic control data and meta information on public and private aircraft. Using a spatio-temporal clustering approach, we demonstrated that interested parties can identify meetings of aircraft belonging to high-profile organizations and governments, using limited training data of known events. Whilst the work uses publicly known events as ground truth, we show that this approach may also reveal private meetings too. At the governmental level, this can highlight relationships between states and/or other entities. For corporations, tracking their aircraft can unearth business intentions and secrets, thus directly affecting their market positions and profits.

Furthermore, our findings show that traditional ways of protecting the privacy of aircraft owners are all but obsolete in the era of cheap software-defined radio receivers and relying on them should be done with extreme caution. We evaluate all existing privacy approaches intended to mitigate the effects of large-scale tracking of non-commercial aircraft: position hiding, pseudonymous identifiers, obscuring aircraft owners and the use or hire of commercial aircraft. Our analysis suggests that whilst they are popular, none are satisfactory. We conclude that a combination of new technical and regulatory measures is required in the long term to protect aviation users' privacy and return it at least to levels seen before the advent of software-defined radios.

References

[1] P. K. Agarwal, J. Erickson, et al. Geometric range searching and its relatives. *Contemporary Mathematics*, 223:1–56, 1999.

[2] B. Blanchet. Symbolic and computational mechanized verification of the arinc823 avionic protocols. In *Computer security foundations symposium (csf), 2017 ieee 30th*. IEEE, 2017, pp. 68–82.

[3] G. Bradley. Coup for Jetstar in Government's $220m travel spend deal as Air NZ yet to be signed up. *New Zealand Herald*, Feb. 2017.

[4] V. Bryan and P. Maushagen. Flightradar24 finds not just planespotters flocking to its website. *Reuters*, May 2015.

[5] D. Cenciotti. Online flight tracking provides interesting details about Russian air bridge to Syria. *The Aviationist*, Sept. 2015. URL: https://theaviationist.com/2015/09/11/ads-b-exposes-russian-air-bridge-to-syria/.

[6] Centro de Observação Astronómica no Algarve. PlanePlotter. 2016. URL: http://www.coaa.co.uk/planeplotter.htm.

[7] K. Close. These CEOs Spend the Most on Corporate Jets for Personal Trips. *Time*, Mar. 2016. URL: http://time.com/money/4250207/ceos-corporate-jets-private-use-barry-diller/.

[8] A. Costin and A. Francillon. Ghost is in the Air(traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. In *Black Hat USA*, July 2012, pp. 1–12.

[9] Council of Europe. European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14. Nov. 1950.

[10] Directorate of Air Traffic Management. Automatic Dependent Surveillance-Broadcast (ADS-B). Tech. rep. New Delhi, India: Airports Authority of India, 2014, pp. 1–10.

[11] P. Dupraz-Dobias. Swiss officials just seized 11 of the world's most expensive cars from this African president's son. *Quartz*, Nov. 2016. URL: https://goo.gl/rR34aP.

[12] European Parliament. Regulation 2016/679 of the European parliament and the Council of the European Union of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/. *Official Journal of the European Communities*, 2016.

[13] Federal Aviation Administration. Aircraft Registry. 2017. URL: https://www.faa.gov/licenses_certificates/aircraft_certification/aircraft_registry/.

[14] Federal Aviation Administration. Equip ADS-B. 2016. URL: https://www.faa.gov/nextgen/equipadsb/.

[15] FlightAware. FlightAware. 2017. URL: https://www.flightaware.com.

[16] FlightRadar24 AB. Flightradar24. 2017. URL: https://www.flightradar24.com.

[17] D. Gloven and D. Voreacos. Dream Insider Informant Led FBI From Galleon to SAC. *Bloomberg*, Dec. 2012. URL: goo.gl/Mf6hbJ.

[18] M. Grabell and S. Jones. Off the Radar: Private Planes Hidden From Public View. *Propublica*, Apr. 2010. URL: https://www.propublica.org/article/off-the-radar-private-planes-hidden-from-public-view-040810.

[19] A. Greenberg. Want To Find Jay-Z's Or Bill Gates' Private Jets? OpenBarr Tracks 'Untrackable' Flights. *Forbes*, July 2012.

[20] B. Hart. Flight Radar Shows Planes Avoiding Ukraine In Aftermath Of Malaysia Airlines Crash. *Huffington Post*, July 2014.

[21] D. Hoffman and S. Rezchikov. Busting the BARR: Tracking "Untrackable" Private Aircraft for Fun & Profit. In *DEF CON 20*. Las Vegas, 2012.

[22] International Civil Aviation Organization. Guidance material on advice to military authorities regarding ADS-B data sharing. Tech. rep. 2012.

[23] *International Standards and Recommended Practices, Annex 10: Aeronautical Telecommunications*. 2nd ed. Volume III: Communication Systems. International Civil Aviation Organization (ICAO), 2nd ed., 2007.

[24] L. Jacinto. Abuse of Power: African Leaders and their Flying Machines. *France 24*, Apr. 2016. URL: https://goo.gl/V4z0Sq.

[25] R. D. Kloth. Airframes.org. 2016. URL: http://www.airframes.org.

[26] A. Laboda. Unencrypted ADS-B OUT Confounds Aircraft Blocking. *NBAA Convention News*, Nov. 2015.

[27] K. Lynch. FAA Exploring Possible Privacy Protections for ADS-B. *AIN Online*, Aug. 2015. URL: http://www.ainonline.com/aviation-news/business-aviation/2015-08-04/faa-exploring-possible-privacy-protections-ads-b.

[28] M. Maremont and T. McGinty. Corporate Jet Set: Leisure vs. Business. *Wall Street Journal*, June 2011.

[29] Minimum operational performance standards for Universal Access Transceiver (UAT) Automatic Dependent Surveillance – Broadcast. Tech. rep. (DO-282B). RTCA, Inc, Dec. 2011.

[30] M. Mitchell, T. Pulvino, and E. Stafford. Price pressure around mergers. *The Journal of Finance*, 59(1):31–63, 2004.

[31] National Business Aviation Administration. Blocking display of Aircraft Situation Display to Industry (ASDI) data. 2017. URL: https://www.nbaa.org/ops/security/asdi/.

[32] OpenFlights. OpenFlights. 2017. URL: https://www.openflights.org.

[33] D. Palan and K. Boldt. Abflug in höhere Sphären. *Manager Magazin*, Apr. 2012. URL: http://www.manager-magazin.de/lifestyle/reise/a-827947-6.html.

[34] K. Sampigethaya and R. Poovendran. Privacy of Future Air Traffic Management Broadcasts. In *28th Digital Avionics Systems Conference (DASC)*. IEEE/AIAA, 2009, pp. 1–11.

[35] K. Sampigethaya, S Taylor, and R. Poovendran. Flight privacy in the nextgen: challenges and opportunities. In *IEEE Integrated Communications, Navigation and Surveillance Conference (ICNS)*. IEEE, 2013.

[36] M. Schäfer, M. Strohmeier, V. Lenders, I. Martinovic, and M. Wilhelm. Bringing Up OpenSky: A Large-scale ADS-B Sensor Network for Research. In *Proceedings of The 13th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, Apr. 2014, pp. 83–94.

[37] M. Schäfer, M. Strohmeier, M. Smith, M. Fuchs, R. Pinheiro, V. Lenders, and I. Martinovic. OpenSky Report 2016: Facts and Figures on SSR Mode S and ADS-B Usage. In *35th IEEE/AIAA Digital Avionics Systems Conference (DASC)*, 2016.

[38] J. Sheridan. Industry Outlines Impediments to Full ADS-B Equipage. *AIN Online*, Dec. 2014. URL: goo.gl/tsy2Rw.

[39] M. Smith, D. Moser, M. Strohmeier, V. Lenders, and I. Martinovic. Economy Class Crypto: Exploring Weak Cipher Usage in Avionic Communications via ACARS. In *International Conference on Financial Cryptography and Data Security 2017*, Apr. 2017.

[40] R. Steele. Open source intelligence. In L. K. Johnson, editor, *Handbook of intelligence studies*, pp. 129–147. Routledge, New York, NY, 2007.

[41] T. Sterling. Dutch bar plane carrying Turkish foreign minister from landing. *Reuters*, Mar. 2017. URL: goo.gl/Ejp7FB.

[42] D. Streufert. ADS-B Exchange. 2016. URL: https://www.adsbexchange.com.

[43] M. Strohmeier, V. Lenders, and I. Martinovic. A k-NN-based Localization Approach for Crowdsourced Air Traffic Communication Networks. *IEEE Transactions on Aerospace and Electronic Systems*, 2018.

[44] M. Strohmeier and I. Martinovic. On Passive Data Link Layer Fingerprinting of Aircraft Transponders. In *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy (CPS-SPC)*. ACM, 2015, pp. 1–9.

[45] M. Strohmeier, M. Smith, M. Schäfer, V. Lenders, and I. Martinovic. Assessing the Impact of Aviation Security on Cyber Power. In *8th International Conference on Cyber Conflict (CyCon)*. NATO CCD COE, 2016, pp. 223–241.

[46] J. Sun. World Aircraft Database. 2016. URL: http://junzisun.com/adb/.

[47] A. Toor. This Twitter bot is tracking dictators' flights in and out of Geneva. *The Verge*, Oct. 2016. URL: http://www.theverge.com/2016/10/13/13243072/twitter-bot-tracks-dictator-planes-geneva-gva-tracker.

[48] G. Topham. Malaysian Airlines plane mystery: how can a flight disappear off radar? *The Guardian*, Mar. 2014. Retrieved on 2017-04-19.

[49] C. Trautvetter. FAA Releases Final Policy on Tail Blocking. *AIN Online*, Aug. 2013. URL: http://www.ainonline.com/aviation-news/business-aviation/2013-08-27/faa-releases-final-policy-tail-blocking.

[50] S. Tully. Can Pope Francis save Alitalia? *Fortune*, Sept. 2015. URL: http://fortune.com/2015/09/20/pope-francis-alitalia-airplane/.

[51] United Nations. Member States. 2017. URL: http://www.un.org/en/member-states/.

[52] US Security and Exchange Commission. Final Rule: Selective Disclosure and Insider Trading. 2000.

[53] T. Webster. Is a war on live flight tracking coming? Retrieved on 2017-04-19. Mar. 2017. URL: https://tonywebster.com/2017/03/war-on-adsb-receivers/.

[54] D. Yanofsky. The confidential list of everyone attending Davos this year. *Quartz*, Jan. 2013. URL: https://qz.com/45509/the-confidential-list-of-everyone-attending-davos-this-year/.

[55] D. Yermack. Tailspotting: identifying and profiting from ceo vacation trips. *Journal of financial economics*, 113(2):252–269, 2014.