Evading the Public Eye: On Astroturfing in Open Aviation Data

Martin Strohmeier, Xavier Olive, Junzi Sun

engineering proceedings

MDPI

Proceeding Paper

Evading the Public Eye: On Astroturfing in Open Aviation Data †

Martin Strohmeier [1,2,*], Xavier Olive [1,3] and Junzi Sun [4]

[1] OpenSky Network, 3400 Burgdorf, Switzerland
[2] Cyber-Defence Campus, Armasuisse Science + Technology, 8005 Zurich, Switzerland
[3] ONERA DTIS, Université de Toulouse, 2, Avenue Édouard Belin, 31055 Toulouse, France
[4] Faculty of Aerospace Engineering, TU Delft, 2619 HS Delft, The Netherlands
* Correspondence: strohmeier@opensky-network.org
† Presented at the 10th OpenSky Symposium, Delft, Netherlands, 10–11 November 2022.

Abstract: The usage of large private and business jets, from those owned by Elon Musk to Kylie Jenner and Bernard Arnault, has recently attracted considerable attention in many countries. Enabled by open and crowdsourced aircraft tracking systems based on the automatic dependent surveillance–broadcast protocol, the aircraft and their owners have been scrutinized. While the underlying technology is not novel and its privacy issues have been discussed for years, the increased attention has led to the backlash against open tracking data and, consequently, a scramble to find possible solutions to hide private jets from the public eye. In this paper, we analyze two such methods, which have not yet been discussed previously in the literature: blocking requests to web tracking platforms and malicious editing of crowdsourced databases. We draw on data from the OpenSky Network and illustrate the futility of such approaches. Finally, we outline the type of stakeholders and aircraft deploying such methods, as well as demonstrate the level of environmental impact that might have otherwise been missed by the public.

Keywords: OpenSky Network; ADS-B; astroturfing; privacy; tracking aircraft emissions; flight environmental cost; business jets

Citation: Strohmeier, M.; Olive, X.; Sun, J. Evading the Public Eye: On Astroturfing in Open Aviation Data. *Eng. Proc.* **2022**, *28*, 7. https://doi.org/10.3390/engproc2022028007

Academic Editor: Michael Schultz

Published: 15 December 2022

1. Introduction

In January 2022, a news story about Elon Musk's aircraft made headlines around the globe. A bot focused on his planes (still operational at https://twitter.com/ElonJet as of 13 December 2022) had started to automatically publish the whereabouts of the aircraft on Twitter using openly available air traffic data. In an alleged attempt to preserve operational security for these planes, Musk made the operator an offer of USD 5000 to take the bot down. The operator, a computer science undergraduate, refused and publicized the attempt, leading to a major global Streisand effect [1].

Following this highly-visible incident, aircraft tracking made headline news several times in the following month. With the beginning of the Ukraine war, interest in military aircraft visible on Flightradar24 and other web trackers increased. Later on, other celebrities besides Musk were caught in the public eye and by climate activists. The private aircraft utilization of stars (from Kylie Jenner to Drake suddenly) became a topic of interest in the United States, culminating in defensive statements by both [2] and further global reporting. In France, business magnate Bernard Arnault's personal and corporate jets became a matter of public debate when an Instagram account based on the API of the OpenSky Network directed attention to their high utilization—and the accompanying climate impact through carbon dioxide emissions [3].

In this paper, we first review the literature and case studies of recent developments on the privacy aspects of ADS-B, in particular with respect to business aircraft in the public view. Secondly, we study two phenomena that have not been addressed so far: the

active suppression of aircraft tracking (a) by directly requesting their exclusion from (live) open data sources and (b) by stealthily attempting to vandalize open aircraft databases. Concretely, we will draw on aggregated and anonymized internal data collected from the OpenSky Network's ticketing system and the algorithms, which build the aircraft database daily.

2. Background

2.1. OpenSky Network

The OpenSky Network is a crowdsourced sensor network collecting surveillance data for air traffic control (ATC). Its objective is to make real-world ATC data accessible to the public and support the development and improvement of ATC technologies and processes. Since 2013, it has continuously been collecting air traffic surveillance data. Unlike commercial flight tracking networks (e.g., Flightradar24 or FlightAware), the OpenSky Network keeps the raw Mode S replies as they are received by the sensors in a large historical database, which can be accessed by academic researchers and analysts.

The non-profit network started with eight sensors in Switzerland and Germany and has grown to more than 5000 registered receivers at locations all around the world. At the time of writing, OpenSky's dataset contains over nine years of ATC communication data. While the network initially focused on ADS-B only, it extended its data range to the full Mode S downlink channel in March 2017 and more recently other technologies, such as FLARM and VHF. The dataset currently contains more than 30 trillion Mode S replies and during peak times receives more than 20 billion messages per day.

More than 300 academic papers have been published to date based on OpenSky data [4]. More information on OpenSky and its many use cases ranging from climate impact to air traffic safety is available in recent OpenSky Reports [5–7].

OpenSky Aircraft Database

As of 1 November 2022, the OpenSky Aircraft Database held 547,924 entries. Monthly snapshots of the database for analysis over time have been taken since December 2019 and are available at https://opensky-network.org/datasets/metadata/ (accessed on 13 December 2022). Figure 1 provides an example of a commercial aircraft owned and operated by SWISS Air.

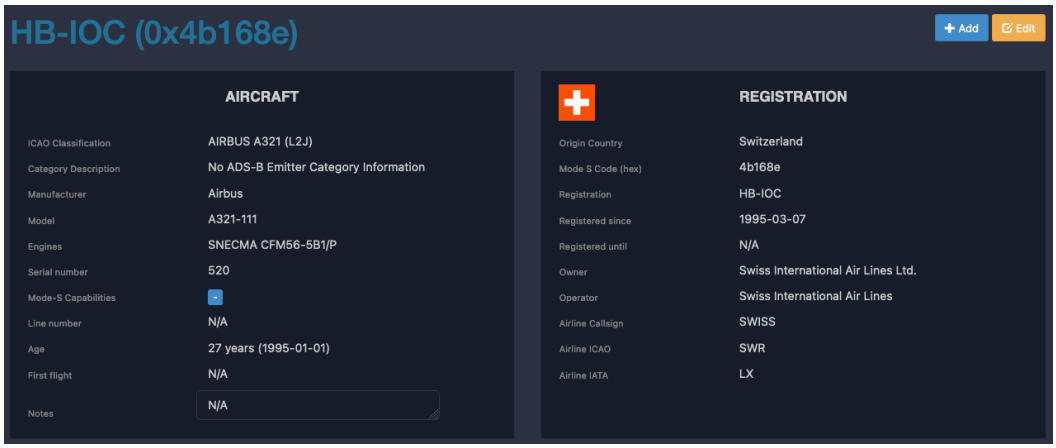

Figure 1. Example of a commercial aircraft entry in the OpenSky database. Add and edit buttons are visible to logged-in users and provide access to the crowdsourcing interfaces.

There are 24 available fields in the database, of which, 22 are editable by users who are registered and logged in (see Table 1). The ICAO24 transponder address as a primary key can only be added for a new aircraft, but not edited later.

Table 1. Fields of the OpenSky aircraft database.

Name	Type	Edit?	Name	Type	Edit?
ICAO24 Code	Primary Key	No	Category	Dropdown	No
Registration	Free Text	Yes	Manufacturer	Free Text	Yes
Registered Since	Date	Yes	Model	Free Text	Yes
Registered Until	Date	Yes	Engines	Free Text	Yes
Owner	Free Text	Yes	Line Number	Free Text	Yes
Operator	Free Text	Yes	Serial Number	Free Text	Yes
Airline Callsign	Free Text	Yes	Built	Date	Yes
Airline ICAO	Free Text	Yes	First Flight	Date	Yes
Airline IATA	Free Text	Yes	Mode S	Checkbox	Yes
Manufacturer ICAO	Free Text	Yes	ADS-B	Checkbox	Yes
ICAO Typecode	Free Text	Yes	ACARS	Checkbox	Yes
ICAO Class	Free Text	Yes	Notes	Free Text	Yes

2.2. Aircraft Privacy

The issue of tracking aircraft has been discussed extensively in the computer security literature, with the conclusion that the ADS-B system does not enable privacy for various stakeholders, due to the unique 24-bit identifier used by aircraft transponders. Several studies examined the privacy and operational security impact of open ADS-B-based tracking on military [8,9], government [9,10], and corporate aircraft [10].

Besides academic analysis, industry bodies and business aircraft stakeholders, such as the National Business Aviation Association (NBAA) in the US, have spoken out for years about the issues concerning their members and advocated for additional protections in the air traffic control system [11]. The only major country and regulator to react to these concerns (at least publicly) has been the Federal Aviation Administration (FAA). Over at least the past 15 years, the issue of mandatory ADS-B transponders has been on the minds of NBAA and FAA, leading to various anti-tracking solutions.

The first and simplest one was a blocking program, first called the block aircraft registration request (BARR), before morphing into the aircraft situation display to the industry (ASDI) and, finally, the limiting aircraft data displayed (LADD). For aircraft on these lists, the dissemination within the FAA's own radar data streams is prevented, as is the display by industry entities such as Flightradar24 or FlightAware. With the advent of cheap and widespread open-source tracking in the 2010s, this approach became obsolete [10].

Beyond these display-based measures, two attempts at changing the underlying technology were made by the FAA. The first was a built-in randomization option of the identifier in the (US-only) universal access transceiver (UAT) data link in the 2000s. The second, called the privacy ICAO address (PIA), started in 2020 and promised random identifiers for the 1090ES data link in the US. Both systems have been shown to be flawed fundamentally as they do not provide any lasting protection [12,13] and are trivially exploited in the wild [14]. Despite this, all discussed approaches remain in popular use, likely because they are the only available options as of today.

2.3. Astroturfing

Astroturfing is a well-known practice in public relations and campaigning where a given message is made to appear as coming from a grassroots source without a conflict of interest and, thus, is perceived as more legitimate.

It has been used widely online and on social media, with academic analysis exposing its use, for example, in politics [15] or against global warming [16]. It is considered an unethical, manipulative tactic, as it is based on deception and often violates formal or informal rules regarding transparency.

3. Astroturfing Attempts in OpenSky

We identified several anonymous OpenSky accounts, which were used in astroturfing attempts in order to change information, such as the registration and owner/operator fields of over 100 aircraft. In our case study, we provide information on the affected aircraft and some background information on the employed accounts.

3.1. Aircraft Database Edits

Overall, 9167 aircraft in the OpenSky aircraft database have seen crowdsourced edits between 24 November 2017 and 12 October 2022 (note that the number of individual edits of the same aircraft cannot be determined from the acquired data). Of these, 8078 or 88.1% were successfully merged in full, i.e., all changed individual fields were merged into the existing database. In 973 cases (10.6%), most changes were denied. Of these 973 cases, in 383 occurrences, no new data were accepted at all. Conversely, in 590 cases, some subsets of data were accepted. In 116 cases (1.3%), there was a conflict regarding the combination of icao24 code and registration fields between the pre-existing data and the user data, in these cases, the user data were consequently rejected as a precaution. This also means that a denied edit in and by itself is not necessarily malicious, however, it serves as a starting point for an investigation.

If we look at edits over time, 455 were made in the complete year of 2018, 984 in 2019, 3204 in 2020, 2295 in 2021, and 2225 in 2022 to date. This indicates a relatively constant editing history over time.

3.2. Analysis of Potentially Malicious Edits

We analyzed those 973 aircraft, where changes were denied, based on their metadata, the timeline of the edits, and the accounts used to do so. We refer to these as suspicious edit attempts from here on.

3.2.1. Utilized Accounts

Suspicious edits were made by 223 different accounts. As noted, a suspicious edit can come from a benevolent account and editing action, as existing verified data cannot be overwritten. As this is not clearly signposted in the OpenSky aircraft database, the likelihood for this to happen over time is high for heavy users with many edits.

Thus, we analyzed the ratio of suspicious edits to successful edits as well as the absolute number of suspicious edits for an account. In absolute terms, 61% or 594 of aircraft where edits were denied came from the top 10 accounts.

We then looked more closely at these 10 accounts and found significant differences in the ratio of suspicious edits to all edits of these users. All the data are shown in Table 2.

Table 2. Number of suspicious edits, sorted by the ratio of suspicious edits to all edits.

Account	% of All Suspicious	# Suspicious	# Overall	Ratio
A1	7.8	76	76	100
A2	3.3	32	43	74.4
A3	4.2	41	68	60.3
A4	8.2	80	214	37.4
A5	5.9	57	158	36.1
A6	3.9	38	138	27.5
A7	8.7	85	938	9.1
A8	2.4	23	307	7.5
A9	12.5	122	2257	5.4
A10	4.1	40	1386	2.9

Consequently, those with high ratios warrant a deeper look at astroturfing activities, although we note that, theoretically, a sophisticated attacker could hide few valuable

malicious edits between many legitimate ones. Through manual inspection we found that accounts A1, A5, and A7 indeed exhibited at least some astroturfing activity, while others inadvertently ran afoul of the database merging rules.

3.2.2. Targeted Aircraft

As we expected much of the targeted astroturfing activity to hide in the long tail of accounts with only one or two edits, we manually inspected all 973 suspiciously edited aircraft for malicious actions. Such actions were loosely defined as deleting or subverting correct and verified data provided by trusted sources. In particular, the deletion or obfuscation of the owner/operator (or all fields) were used as a signal.

Based on these rules, 170 aircraft were deemed targets of astroturfing. Only 6 of these aircraft were commercial airliners, which is not surprising as they are of low interest in the larger privacy discussion. Here, the intent may have been benign or simply 'normal' vandalism. The vast majority (114) were larger corporate/business jets, followed by 41 smaller private aircraft; 5 were governmental, 1 military, 1 aerial surveillance, and 2 aircraft belonged to emergency services.

As would be expected from these stakeholders, the distribution of aircraft types is skewed heavily toward Bombardier Challengers (16), Dassault Falcons (13), and Gulfstreams (50). Regarding origin countries, 83 aircraft were registered in the US, 28 in Australia, 17 in the UK, 16 in Canada, and 7 in Switzerland. Note that the lack of verified non-user data in some countries, such as Germany or France, may make it more difficult to notice malicious edits automatically for aircraft registered there.

3.2.3. Astroturfing Case Studies

We now provide some details on the most egregious activity we uncovered.

- Targeted hiding of French business aircraft:
  This study was initially motivated by data collection on high-profile business aircraft and their carbon dioxide impact [17]. We discovered that a freshly registered user added a non-existing Air France aircraft to the transponder ID 395580 (see Figure 2). This ID was actually registered to LVMH services GIE, at the time under much scrutiny in the public media for their use of business jets—uncovered by the use of the OpenSky API [3].
- The top astroturfing account:
  A manual investigation of the top account from Table 2 shows that indeed all 76 attempts can be classified as perceived astroturfing. In all cases, the data pertaining to manufacturername, model, serialnumber, operator, owner, registered, built, and engines were deleted where they existed. Curiously, in 43 cases, no data beyond the mere existence of the aircraft had previously been recorded in the database. We speculate that the account, therefore, likely worked off a list provided to them. Incidentally, the list included the ICAO24 ID 395588 (registration F-GVMI) also registered to LVMH Services Gie. All targets were large business jets, used by private individuals, as far as it was possible to investigate using open-source material.
  The first suspicious edit was made on 12 December 2021 at 03:29:56 (UTC). At the time of data collection, the edits were ongoing with the last edit made on 16 September 2022 at 14:41:34. Thus, the action was ongoing for more than 9 months. The user registered on 10 December 2021 at 00:53:06 with a throwaway email address, a six-digit number at the Swiss provider Protonmail, whose advertising focuses on security and privacy and Switzerland's strict privacy laws.

Successful merge			
icao24	395580	395580	395580
registration	F-HJJI	F-HJJI	F-HJJI
timestamp	1970-01-01 01:00:00.0	2022-06-19 06:07:40.0	2022-06-19 06:07:40.0
source	null	user-data	user-data
manufacturericao		AIRBUS	AIRBUS
manufacturername		AIRBUS	AIRBUS
model		A321 NEO	A321 NEO
typecode		A321	A321
serialnumber		255578	255578
operator		Air France	Air France
operatorcallsign		AIRFRANS	AIRFRANS
operatoricao		AFR	AFR
operatoriata		AF	AF

Figure 2. Astroturfing event. A non-existing Air France aircraft with registration `F-HJJI` is added to the transponder ID `395580`, then registered to LVMH Services GIE. Previously, there were no data in the database.

4. Blocking Requests in OpenSky

We now draw on aggregated and anonymized internal data collected from the OpenSky Network's ticketing system. Over the past 5 years, OpenSky has received 73 requests from various stakeholders inquiring about the removal of their aircraft from the public eye. We do not dwell on the legitimacy of such undertakings (and disregard the absolute futility as discussed previously in [10]) but instead focus on the type of stakeholders interested in such actions. Note that OpenSky never compromises the integrity of the data available to researchers in its databases, which is always raw and complete. OpenSky may request the anonymization of published data in line with the requirements of the ethics committees and scientific journals.

Discarding duplicate requests and broader inquiries about the process without identifying plane details, this leaves 39 attempts at removing concrete aircraft from the view of the public and scientists. Since many of such requests pertain to several aircraft, a total of 92 tail numbers were implicated, which we subsequently analyze.

These aircraft come from four different backgrounds: privately used aircraft (24), charter services (15), corporations (18), and authorities, such as local or federal governments (35). Slicing it by country, the top countries with at least 3 requested aircraft are Saudi Arabia (18 aircraft), USA (12), Germany (10), Slovenia (7), Russia (7), Poland (6), Malta (6), Brazil (4), Venezuela (3), Finland (3).

We can only speculate about the true reason for any particular blocking request but the general motives are known from previous research and communication by industry bodies. Some non-celebrity owners have strong feelings about privacy, and some celebrities fear for their operational security (OPSEC). Police and coastguard forces, or presidents and royal families, may also have legitimate OPSEC reasons. However, we also want to note that many aircraft on the list have been implicated in international sanctions on their oligarch owners and may seek to avoid legal and public scrutiny.

No matter the motives, the futility of such privacy through obscurity has been discussed at length in the literature [9,10]. Blocking aircraft from web trackers is a measure that was partially effective in the 2000s but with the advent of ubiquitous crowdsourced ADS-B reception and sharing, it provides no additional OPSEC or privacy. Under no circumstances should police forces in particular rely on this, they should always assume their tracks are easily and widely accessible.

On the contrary, such requests can make an aircraft more interesting, as it can stick out like a sore thumb. The official "Limiting Aircraft Data Displayed" (LADD) (https://www.faa.gov/pilots/ladd accessed on 13 December 2022) list of the FAA can be obtained via reverse engineering or through freedom of information requests. Filters for aircraft on this particular list are then offered for example on adsbexchange.com, contravening the original intent in its entirety. Among the OpenSky block requests, this is showcased for example by the block request of a large petroleum company days before they used the aircraft to fly to merger negotiations, a signal of potential value on the stock market [10].

5. Calculating the Climate Impact Hidden by Flight Blocking

To demonstrate the impact of potential blocking requests on climate research and public scrutiny, we analyze the flight distance and estimated total emissions of the aircraft implicated in these requests. 67 of the 92 could be seen flying in OpenSky's coverage region during 2021, resulting in 4592 flights. Figure 3 shows the total flight distance recorded. We also show the CO_2 emission estimated for the flights carried out by these aircraft using the OpenAP model [18]. While we cannot be sure in which cases specifically "climate guilt" and public shaming over the high per-capita emissions of private jets were the primary drivers for the blocking requests, it is likely to be an issue for several of them, judging by the timing of their requests and media reporting.

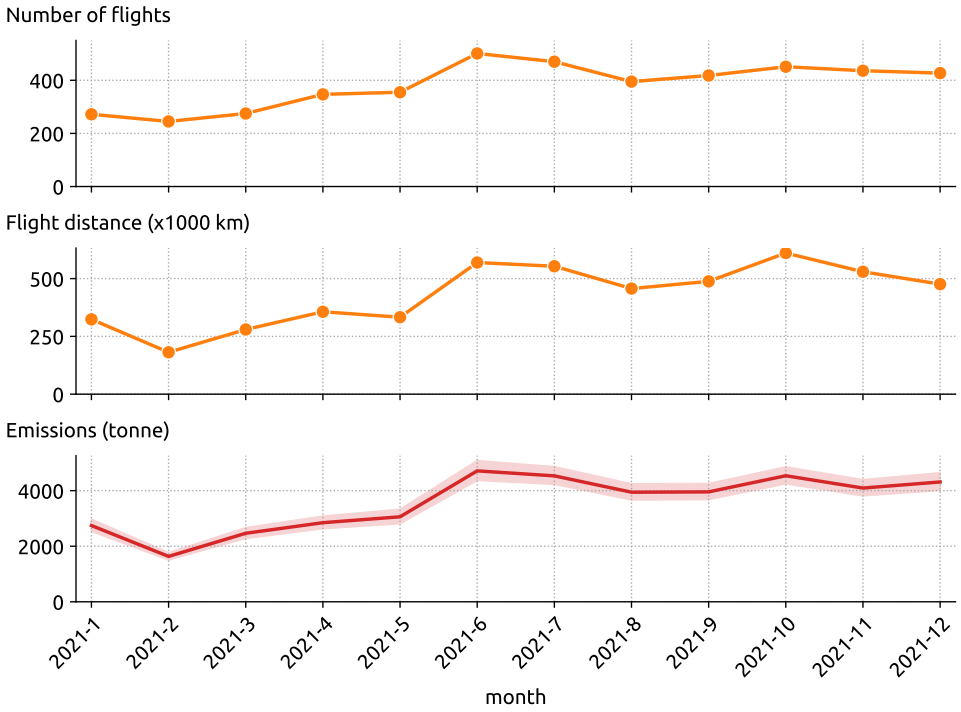

Figure 3. Total flights, distance, and emissions caused by 67 aircraft that requested to be removed from OpenSky over the year 2021.

6. Countermeasures

The problem of astroturfing is not novel but is known in many crowdsourced databases. Fundamentally, there are two types of countermeasures: algorithmic and user-centric.

6.1. Algorithmic Detection

In the following, we briefly describe OpenSky's current method of re-building the crowdsourced aircraft database daily. While this algorithmic approach was not strictly intended to cope with sophisticated astroturfing attempts, it still serves successfully as both a defense against vandalism and a detection mechanism.

The database is built from various input data according to the following precedence:

1. The highest precedence (0) is given to original, verified data sources, such as national aircraft registries openly available (e.g., US FAA, Canadian, Swiss, or UK Civil Aviation Authorities). These are typically updated regularly from the source.
2. Second highest precedence (1) is given to the data of aircraft seen via ADS-B. This includes only the ICAO24 transponder code and the category, both of which are broadcast by the aircraft itself. If there are no other data, this serves as a basic seed.
3. Lowest precedence (2) is given to direct edits by users on the website as well as all crowdsourced data collections (e.g., 'basestation.sqb' files) available on the internet

and shared with OpenSky. OpenSky considers all such inputs as crowdsourced data, thus assigning the same precedence.

In case of conflicts and an equal precedence level value, data with the most current timestamp will have precedence unless a field is empty. In effect, the described setup means that user data are 'append only' with regard to all non-user supplied data. Official registry data cannot be overwritten, only other user data.

6.2. Active and User-Centric Curation

On the side of user-centric countermeasures, OpenSky could give trusted and verified persons a higher priority and/or special editing rights. This would follow a model that is practiced, for example, by Wikipedia. Other options along these lines would include publishing the change logs for public scrutiny. Currently, only OpenSky's administrators can check these logs and identify malicious edits. Finally, known controversial aircraft could be locked, preventing edits by anyone not trusted to do so. In conjunction, these measures have proven to be highly effective against malicious edits even at the largest scale, and are recommended for inclusion in OpenSky in the future.

7. Discussion

7.1. Requirement for Privacy in Aviation

The Musk case is highly illustrative, as money was offered to take a Twitter bot down (a futile attempt, as it is based on openly available data). Secondly, the PIA was implemented—a futile attempt, as the underlying system is not secure and was quickly side-stepped even by a first-year computer science student without much effort.

Likewise, many other celebrities suddenly felt the public pressure and the need to justify their private flights in a changing environment. All of this illustrates the need for privacy as codified by the NBAA and the FAA in the various described attempts (see Section 2.2). Unfortunately, it is also becoming more clear that the existing aviation infrastructure simply does not allow for the privacy of private jets.

This reality seems to set in for some state actors at least. The Canadian government has first issued (and then in short order reversed) a decision for their air transport service to be hidden from web trackers using the LADD blocklists [19].

7.2. Counter-Intuitive Effects of Astroturfing

While our study is only a first attempt at analyzing covert attempts at thwarting open data aircraft tracking, it is already clear that it can easily have effects that are counter-intuitive or even paradoxical in the medium term. Naturally, it is difficult to estimate how many attempts have gone successfully unnoticed (and for how long). Still, in many cases trying to hide evidence is (a) only the initial reason why someone would notice a certain aircraft's activity in the first place (after all, there are millions of flights every month in which one can hide) and (b) increase the interest in this activity, if it is deemed worth hiding by the owner/operator. Such Streisand effects on the internet are well-known in the literature and have been discussed under this name since 2003 [20].

7.3. Social Media as Scale Multiplier

The basis for Twitter bots and other means of publicly tracking specific aircraft is the existence of open, crowdsourced ADS-B and aircraft data. Since attempts at suppressing ADS-B data from the web have proven futile, there have been many attempts to suppress coverage of specific aircraft of interest. In connection with the aforementioned Streisand effects, we can observe that many attempts to cover or deny aircraft activities only lead to large-scale attention on social media, which is often followed by even greater attention through traditional media outlets.

7.4. Integrity Attacks on Other Aircraft Trackers

Other unfiltered (as advertised by the operators but not verified independently) web trackers such as ADS-B Exchange are also widely used to track the same aircraft. Successful attempts at subverting the data have been reported in those cases, e.g., by directly feeding bogus military aircraft data into the Taiwan airspace view during the widely-watched visit of Nancy Pelosi in August 2022 (https://twitter.com/vcdgf555/status/1554301925897617408, accessed on 13 December 2022). Issues with ADS-B data integrity due to its unauthenticated nature have been known for a long time and discussed in detail by Schäfer et al. [5]. At a minimum, a sensor registration should be instituted by any web tracker that cares about data integrity.

8. Conclusions

Aircraft tracking using open data, in particular of corporate and celebrity planes, has seen increased attention in 2022. We have shown that some actors use methods of astroturfing and malicious interference with open databases in order to make such tracking harder and in some cases mask their controversial climate impact. We analyzed actors, targets, and climate impact using data from the OpenSky Network. In light of the distributed nature of modern aircraft tracking on the internet, we argue that this approach is futile in the long run. Yet, researchers should pay attention in the short term before using data involving potentially controversial aircraft.

Author Contributions: Conceptualization, M.S. and X.O.; methodology, M.S.; software, J.S.; validation, M.S., X.O. and J.S.; formal analysis, J.S.; investigation, M.S.; data curation, M.S.; writing—original draft preparation, M.S.; writing—review and editing, X.O. and J.S.; visualization, J.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: OpenSky aircraft database is available at https://opensky-network.org/aircraft-database. Aircraft flight tracks are available at https://opensky-network.org.

Acknowledgments: We thank the OpenSky Network for their help and tailored data access. In particular, we thank Marco Meides for his time in implementing and explaining the aircraft database.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Irwin, V. A 19-Year-Old Built a Flight-Tracking Twitter Bot. Elon Musk Tried to Pay Him to Stop. *Protocol*, 26 January 2022. Available online: https://www.protocol.com/elon-musk-flight-tracker (accessed on 13 December 2022).
2. Chiu, A. Celebrities Use Private Jets Excessively. It's a Climate Nightmare. *Washington Post*, 2 August 2022. Available online: https://www.washingtonpost.com/climate-environment/2022/08/02/taylor-swift-kylie-jenner-private-jet-emissions/ (accessed on 13 December 2022).
3. Sauvage, G. Le "Flight tracking" des Milliardaires, Outil Pour déNoncer les Injustices climatiques. *France24*, 8 August 2022. Available online: https://f24.my/8orQ (accessed on 13 December 2022).
4. Strohmeier, M. Research Usage and Social Impact of Crowdsourced Air Traffic Data. In Proceedings of the 8th OpenSky Network Symposium, Online, 12–13 November 2020; Volume 59, p. 1.
5. Schäfer, M.; Strohmeier, M.; Smith, M.; Fuchs, M.; Lenders, V.; Martinovic, I. OpenSky Report 2018: Assessing the Integrity of Crowdsourced Mode S and ADS-B Data. In Proceedings of the 2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC), London, UK, 23–27 September 2018; pp. 1–9.
6. Sun, J.; Olive, X.; Strohmeier, M.; Schäfer, M.; Martinovic, I.; Lenders, V. OpenSky Report 2021: Insights on ADS-B Mandate and Fleet Deployment in Times of Crisis. In Proceedings of the 2021 IEEE/AIAA 40th Digital Avionics Systems Conference (DASC), San Antonio, TX, USA, 3–7 October 2021; pp. 1–10.
7. Sun, J.; Basora, L.; Olive, X.; Strohmeier, M.; Schäfer, M.; Martinovic, I.; Lenders, V. OpenSky Report 2022: Evaluating Aviation Emissions Using Crowdsourced Open Flight Data. In Proceedings of the 2022 IEEE/AIAA 41st Digital Avionics Systems Conference (DASC), Portsmouth, VA, USA, 18–22 September 2022; pp. 1–10.

8. Schäfer, M.; Strohmeier, M.; Smith, M.; Fuchs, M.; Lenders, V.; Liechti, M.; Martinovic, I. OpenSky report 2017: Mode S and ADS-B usage of military and other state aircraft. In Proceedings of the 2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC), St. Petersburg, FL, USA, 17–21 September 2017; pp. 1–10.
9. Strohmeier, M.; Smith, M.; Moser, D.; Schäfer, M.; Lenders, V.; Martinovic, I. Utilizing air traffic communications for OSINT on state and government aircraft. In Proceedings of the 2018 10th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 29 May–1 June 2018; pp. 299–320.
10. Strohmeier, M.; Smith, M.; Lenders, V.; Martinovic, I. The real first class? Inferring confidential corporate mergers and government relations from air traffic communication. In Proceedings of the 2018 IEEE European Symposium on Security and Privacy (EuroS&P), London, UK, 24–26 April 2018; pp. 107–121.
11. National Business Aviation Association. *NBAA Examines Privacy in the ADS-B Era*; National Business Aviation Association: Washington, DC, USA, 2022.
12. Sampigethaya, K.; Taylor, S.; Poovendran, R. Flight privacy in the NextGen: Challenges and opportunities. In Proceedings of the 2013 Integrated Communications, Navigation and Surveillance Conference (ICNS), Herndon, VA, USA, 22–25 April 2013; pp. 1–15.
13. Michel, G.; Strohmeier, M. Flying in Private Mode: Understanding and Improving the Privacy ICAO Address Program. *J. Aerosp. Inf. Syst.* **2021**, *18*, 530–538. [CrossRef]
14. Askeland, S. PIA privacy program no match for teen tracking Elon Musk's Gulfstream on Twitter through ADS-B data. GlobalAir.com, 31 January 2022. Available online: https://www.globalair.com/articles/pia-privacy-program-no-match-for-teen-tracking-elon-musks-gulfstream-on-twitter-through-ads-b-data?id=4209 (accessed on 13 December 2022).
15. Keller, F.B.; Schoch, D.; Stier, S.; Yang, J. Political astroturfing on Twitter: How to coordinate a disinformation campaign. *Political Commun.* **2020**, *37*, 256–280. [CrossRef]
16. Cho, C.H.; Martens, M.L.; Kim, H.; Rodrigue, M. Astroturfing global warming: It isn't always greener on the other side of the fence. *J. Bus. Ethics* **2011**, *104*, 571–587. [CrossRef]
17. Sun, J.; Olive, X.; Strohmeier, M. Environmental Footprint of Private and Business Jets. In Proceedings of the 10th OpenSky Network Symposium, Delft, The Netherlands, 10–11 November 2022.
18. Sun, J.; Hoekstra, J.M.; Ellerbroek, J. OpenAP: An open-source aircraft performance model for air transportation studies and simulations. *Aerospace* **2020**, *7*, 104. [CrossRef]
19. Passifiume, B. Ottawa reverses order to block PM's flights from tracking websites. nationalpost.com, 5 October 2022. Available online: https://nationalpost.com/news/politics/ottawa-reverses-order-to-block-pms-flights-from-tracking-websites (accessed on 13 December 2022).
20. Jansen, S.C.; Martin, B. The Streisand effect and censorship backfire. *Int. J. Commun.* **2015**, *9*, 656–671.