DE GRUYTER OPEN Proceedings on Privacy Enhancing Technologies ; 2018 (3):105–122

Matthew Smith*, Daniel Moser, Martin Strohmeier, Vincent Lenders, and Ivan Martinovic

Undermining Privacy in the Aircraft Communications Addressing and Reporting System (ACARS)

Abstract: Despite the Aircraft Communications, Addressing and Reporting System (ACARS) being widely deployed for over twenty years, little scrutiny has been applied to it outside of the aviation community. Whilst originally utilized by commercial airlines to track their flights and provide automated timekeeping on crew, today it serves as a multi-purpose air-ground data link for many aviation stakeholders including private jet owners, state actors and military. Such a change has caused ACARS to be used far beyond its original mandate; to date no work has been undertaken to assess the extent of this especially with regard to privacy and the various stakeholder groups which use it.

In this paper, we present an analysis of ACARS usage by privacy sensitive actors—military, government and business. We conduct this using data from the VHF (both traditional ACARS, and VDL mode 2) and satellite communications subnetworks. Based on more than two million ACARS messages collected over the course of 16 months, we demonstrate that current ACARS usage systematically breaches location privacy for all examined aviation stakeholder groups, explaining the types of messages used to cause this problem. We illustrate the challenges with three case studies—one for each stakeholder group—to show how much privacy sensitive information can be constructed with a handful of ACARS messages. We contextualize our findings with opinions on the issue of privacy in ACARS from 40 aviation industry professionals. From this, we explore recommendations for how to address these issues, including use of encryption and policy measures.

Keywords: aviation privacy, ACARS, avionic systems

DOI 10.1515/popets-2018-0023

Received 2017-11-30; revised 2018-03-15; accepted 2018-03-16.

***Corresponding Author: Matthew Smith, Martin Strohmeier, Ivan Martinovic:** Department of Computer Science, University of Oxford: first.last@cs.ox.ac.uk

Daniel Moser: Department of Computer Science, ETH Zurich: first.last@inf.ethz.ch

Vincent Lenders: armasuisse: first.last@armasuisse.ch

1 Introduction

The aviation industry's strong focus on safety has brought about the continued use of a multitude of proven legacy communication technologies developed several decades ago. One significant example is the Aircraft Communications, Addressing and Reporting System (ACARS), which provides data link communications between aircraft and entities on the ground and is used for many different purposes, from the management of aircraft fleet to air traffic control (ATC) [34].

As with many areas of transport, aviation strives to become more 'connected', utilizing wireless data link technologies to improve efficiency. Anecdotally, the way the ACARS data link is being used has significantly changed over time. Whilst originally used by commercial airlines to track their flights and provide automated crew timekeeping, today it serves as a multi-purpose air-ground data link for many stakeholders including private jet owners, state actors and military.

Using only a basic ASCII character set and operating in a similar way to SMS messaging, ACARS defines several message formats and protocols to provide a range of different services. As the system was not designed with security in mind and offers no confidentiality by default, the vast majority of ACARS traffic is still in the clear and can be trivially intercepted using cheap software-defined radios (SDRs) and software freely obtained on the Internet (e.g., ACARSDec [29]).

This has not been the case until relatively recently; receiving ACARS required specialist hardware and software, if it was even obtainable by those outside of aviation at all. The introduction of SDRs, specifically cheaper and readily available units, has created an active community of developers building tools to decode aviation communication signals, amongst others. This has brought ACARS from being a difficult-to-access medium to accessible by ordinary computer users.

Concerns about the clear-text nature of ACARS have been highlighted from individuals within the aviation community as far back as 1998 [57]. Recently, an ex-pilot discussed his view of ACARS usage from the cockpit, acknowledging the eavesdropping threat and providing anecdotes of messages circulated widely despite being intended for a narrow group of people [37]. Recent assessments from the Airline Pilot's Association [5] and the US Air Force [8] assert that message injection with false information is a realistic threat.

Despite these concerns and its global deployment, the usage of ACARS with respect to privacy has not been studied. In this paper we present a first such measurement study into the location privacy problems caused by ACARS usage. Our findings show that there is a significant leakage of privacy-sensitive data on the ACARS channel. Messages which initially appear innocuous can leak significant amounts of information, especially for stakeholders who otherwise demonstrate a desire for privacy. Usually, these actors try to hide flight information—ACARS messages are regularly undermine this effort. We further surveyed 40 aviation industry professionals to assess the extent to which they believe ACARS offers reasonable privacy and safety, finding that 77.5% of respondents do not find ACARS suitable for private data.

Privacy in aviation is a concept defined from schemes which exist to protect it; a lack of by-default security means few technical measures are in use. We use the actions of aircraft owners or operators attempting to obscure themselves from public sources of flight data as a firm indication of sought privacy. In some countries, governmental schemes exist to 'block' aircraft from these feeds, whereas elsewhere an owner needs to contact flight trackers individually. Within our collection we that observed 92% of business, 64% of military and 96% of government aircraft seen have some block in place on public dissemination of aircraft information.

Usually, public flight data would reveal the location and historical flight movements, thus tied to location privacy. We consider 'blocking' of an aircraft on public data feeds to be a specific effort to provide privacy to the owner or operator. Since these feeds use surveillance—rather than data link—technologies, ACARS provides an out-of-band view.

Contributions

Our contributions are as follows:

- We collect and analyze the message content of 2,760,141 messages collected over 16 months, correlating it with public aircraft metadata sources.
- We demonstrate the privacy issues caused to business, military and government aircraft as a result of ACARS usage, categorized by the type of ACARS message and with case studies.
- We contextualize the findings with survey results, collecting the opinions of aviation professionals involved with ACARS.
- We analyze the implications of sensitive ACARS data link usage, especially with respect to how it evolved over time, and discuss possible mitigations.

The paper is structured as follows. We begin by introducing aviation and ACARS in Section 2 before devising a threat model in Section 3 and explaining our data collection methodology in Section 4. We briefly describe the aircraft categories of interest in Section 5, before looking at the concept of blocking aircraft movements in Section 6. We explore the privacy issues for blocked aircraft caused by ACARS in Section 7 and use case studies to elaborate on this in Section 8. We go on to look at industry opinions in Section 9, then discuss mitigations in Section 10. Finally, we look at the related work in Section 11 before concluding.

2 Background

In this section, we introduce the key concepts needed to contextualize the problem of sensitive data leakage from ACARS. We first explain the aviation scenario before looking at ACARS and how it is used in detail.

2.1 Aviation

Airspaces are complex, safety-critical environments which rely on quick, accurate communication. Each country or region has Air Navigation Service Providers (ANSPs) which administer ATC for their area. They are responsible for ensuring that aircraft have separation, allocating take-off and landing slots, and handling arising emergencies. In order to do this, voice and data communications are used extensively both on the ground and in the air. Furthermore, aircraft operators monitor information such as location, estimated arrival times and maintenance data allowing for faster turnarounds and efficient operation.

A number of systems are used to manage the civil airspace with future developments focusing on data link rather than voice communications. This involves introducing systems such as Automatic Dependent Surveillance-Broadcast (ADS-B) for tracking aircraft [13], making greater use of Secondary Radar to provide situational awareness (see [45]) as well as utilizing existing systems such as ACARS until new ones are deployed.

For the purposes of this paper, we specifically consider non-commercial, non-hobbyist aviation. Commercial aircraft (i.e. airlines operating large aircraft as a business, and open to the public) operate in a transparent fashion with respect to data links. Whether this is a reasonable choice is considered out-of-scope for this paper. Non-commercial aircraft are heterogeneous in type and user so use data link in many ways, not all of which would be public. We further explain the categories used in Section 5.

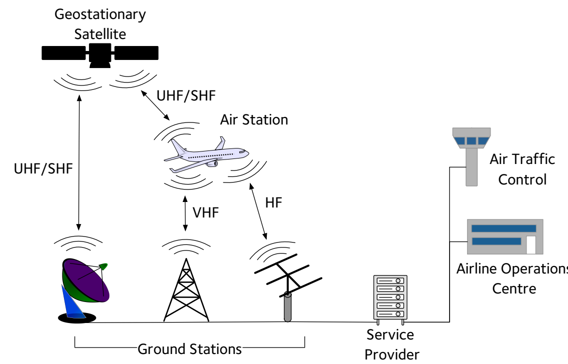

Fig. 1. The ACARS sub-systems.

2.2 Aircraft Communications Addressing and Reporting System

Originating from the VHF network created in 1978 [35], ACARS provides an ASCII character-based data link between aircraft and ground stations defined by ARINC 724B-6 [3]. Originally specified for Very High Frequency (VHF), new High Frequency (HF) and Satellite Communications (SATCOM) links were added, allowing worldwide coverage. Typically, VHF is used over populated land, SATCOM extends coverage to oceanic and rural land areas, and HF provides coverage worldwide.

VHF is offered through a technology known as Plain Old ACARS (POA) and the newer VHF Data Link mode 2 (VDLm2) offering a higher data rate. SATCOM provides several channel groups with different bit rates, depending on the constellation used. Two main providers exist; Inmarsat and Iridium. Typically, higher bit rate channels cost more to use. A representation of the ACARS subsystems can be seen in Figure 1. An aircraft will select one of the three communication methods based on signal strength—typically, the priority from high-to-low is VHF (POA/VDLm2), SATCOM and HF.

ACARS messages are mainly composed of 210 character text field, with routing to an aircraft achieved via a flight ID (i.e. flight number). Messages have a 'label', used by a Communications Management Unit (CMU), to send the content to the correct on-board system. Message content itself is structured according to the ARINC 620-8 standard [4]. Many message types are defined to cover a wide range of purposes including weather reports, aircrew free-text messages or time updates. Naturally, messages of different purposes will be originated by different devices on board or on the ground.

2.3 Usage of ACARS

Many aircraft systems originate ACARS messages, creating a range of information types sent over the link. Most services provided now were not part of the system's original intention—ACARS was initially designed to log the hours worked by crew [35]. It has evolved significantly, with some example uses stated below:

ATC Clearance. Aircraft use a predefined ACARS message exchange protocol, e.g. to make requests to change or extend the assigned route; typically this is used in limited coverage areas such as the ocean. When used it is the default (instead of voice) and aids in reducing congestion on voice channels.

Information Services. In order to handle changes en route due to weather or local restrictions which occur in-flight, ACARS can be used to retrieve up-to-date information via data link.

Flight Plans. Airlines will often transfer flight plans including routes, destination and loading information to aircraft ahead of departure.

Positional Reports. Although ACARS is not primarily intended for position reporting, in particular since the introduction of ADS-B, some aircraft do use it. Generally, these messages are consistent in form and contain origin and destination information as well as position.

Diagnostic Feeds. To track required maintenance on aircraft systems, some components such as engines automatically report their status to the manufacturer. This is primarily used by commercial aircraft, so we do not consider it further.

Free-text Messages. Often, the staff needs to communicate outside of the constraints of structured ACARS messages, from requests for medical aid to sports scores.

Naturally, some ACARS users are more privacy-sensitive than others. Means exist to obscure or limit public dissemination of data about flights of such users, of which we explore further in Section 6. Of the above message types, this paper focuses on the particularly privacy sensitive types: location reports, flight plans and information services. These are covered in detail in Section 7.

3 Threat Model

To frame our discussion, we first introduce the observed threat to users of avionic data link systems. With respect to the medium, we consider a fully passive attacker, who only receives messages.

Due to the general lack of security in ACARS the barrier-to-entry for an attacker is low. We presume an attacker to be moderately resourced, having access to standard desktop computers, commodity software-defined radios (SDRs) and antenna. We further presume a moderate level of technical capability, i.e. the attacker can set up and use the equipment, with the ability to produce tools to operate the SDR. Given the range of uses for avionic data link, different attackers are likely to have varying intentions. Primarily, we model an attacker collecting data for either criminal gain, to achieve competitive advantage, or conduct a form of surveillance.

Attackers seeking criminal gain might focus on financial or operational data allowing them to steal assets or blackmail victims. Those looking for competitive advantage might seek to track corporate aircraft to predict business actions. Threat actors aiming to use data link for surveillance may want to know if an aircraft is in the air, others might want to acquire more detailed information about its location and status. Although we replicate a modest attacker in this paper, we expect that more determined attackers could scale up such a setup to collect more data with only limited extra cost.

4 Methodology

To measure ACARS usage, we used a combination of first-hand data collection and third-party data sources. This section explains our approach to this collection and the criteria we use to categorise aircraft in our analysis.

4.1 ACARS Collection

For a long time after conception ACARS required specialist hardware to decode, as described above. Recently, software-defined radios such as the RTL-SDR have become available for as little as $10, spurring the development of software enabling the decoding of previously specialist communications. A number of tools exist to decode ACARS, many of which are free. We focus on VHF (POA and VDLm2) and SATCOM as these are the most heavily utilized ACARS subnetworks.

VHF

The VHF downlink is comprised of POA and VDLm2 ACARS. A typical POA setup is requires an airband antenna fed into an RTL-SDR running ACARSDec [29]. We collected for 141 days (May-Oct. 2016) followed by a further 220 days (Mar.-Oct. 2017) on the three European channels: 131.525 MHz, 131.725 MHz and 131.850 MHz. We also collected VDLm2 ACARS messages in a separate collection period for 211 days (Mar.-Oct. 2017) over five European frequencies: 136.725 MHz, 136.775 MHz, 136.875 MHz and 136.975 MHz. This was collected from a central European country.

SATCOM

The SATCOM uplink is located in the L-band around 1.5 GHz; reception uses a patch antenna fed into an RTL-SDR running JAERO [36]. We recorded all 11 uplink channels of INMARSAT satellite 3F2 for 68 days between November 2016 and January 2017.

Uplink messages use higher power and lower wavelengths than downlink due to aircraft having limited receiver space; this can be intercepted with a patch antenna as the beam area is large. Downlink, located in the C-band around 3.5 GHz, has much shorter wavelengths and increased path loss. Ground stations receiving downlink can use bigger receivers than aircraft, allowing satellites to transmit at higher wavelength thus having a smaller beam and requiring third parties to use a large satellite dish to intercept. As such, we only collect uplink for SATCOM.

4.2 Collection Statistics

Over the course of collection, we obtained 2,760,165 messages across both links, with 1,170,040 (42.4%) being from SATCOM uplink, 1,059,608 (38.4%) on VDL mode 2 and the remaining 530,517 (19.2%) being POA. We registered 9924 individual aircraft, of which 6184 were seen over POA, 4817 over VDLm2 and 4529 on the SATCOM channels. A total of 430 aircraft were seen over all three links and 2631 were transmitting on both terrestrial transmission technologies. We look at further aircraft statistics per category in Section 5.

4.3 Aircraft Positional Data

In some instances, we observe aircraft sending privacy-sensitive ACARS messages without location. The OpenSky Network [44] provides high-quality historical ADS-B data, covering our ACARS collection period. As a contributor to the network we can use ADS-B data collected from across the world to check whether an aircraft was transmitting ADS-B signals at the time, and if so, its position. In places where we cross-reference, we indicate it explicitly.

4.4 Aircraft Meta Data Sources

To asses the extent to which data transmitted is sensitive, we require sources—ideally publicly accessible—to compare with our ACARS data. Many meta-information sources on aircraft exist, based on their identifiers. This is usually the aircraft registration or a unique 24 bit address provided by the International Civil Aviation Organization (ICAO). This information typically includes the aircraft type (e.g., Airbus A320) and the owner/operator (e.g., British Airways, but the owner and operator may not always be the same). We use this to categorize the aircraft and assess its privacy requirements. Several public databases provided by third parties are used for these purposes:

- We check whether the aircraft are visible on the flight tracker FlightAware [15].
- We compare against all visible aircraft on Flightradar24 using a database created by Junzi Sun [53].
- Airframes.org offers background knowledge such as pictures and historical ownership data [28].
- Under a Freedom of Information Act request, the full BARR list of blocked aircraft was provided [56]. This will be covered in Section 6.
- For US-registered aircraft, the FAA provides a daily updated database of all non-sensitive owner records.

4.5 Survey of Industry Opinions

As a global industry, aviation is comprised of many stakeholders with their own interests. To better understand how this affects ACARS usage, we conducted a survey to gather the opinions from aviation professionals. We use this information to provide context to our findings and explore the ground truth relating to privacy in ACARS. The survey was distributed to both public and private pilot, air traffic controller and avionic engineer communities, collecting responses anonymously over the course of six weeks. During this time we had 40 responses. We expand on our results in Section 9, but where relevant discuss them throughout the paper.

4.6 Legal and Ethical Considerations

Since we were aware that the likelihood of collecting sensitive data was high we upheld strong ethical conduct throughout the work. At all times data access was restricted and not disseminated in full form. Indeed, we have made great efforts to anonymize data presented in this paper such that the privacy breach cannot be exploited through our work. We ensure that no identity data is present with respect to comments about specific aircraft, and do not provide dates beyond month and year for when flights occurred. We ensured that all relevant laws and regulations were adhered to. On top of this, our survey was conducted anonymously, in compliance with data protection laws and with ethical approval R53464/RE001.

5 Aircraft Categories

The aviation ecosystem has a diverse set of stakeholders. We are particularly interested in stakeholders with a desire for privacy, who we describe in this section. As mentioned above, we focus on military, business and government aircraft as their ACARS usage is similar. Commercial aircraft have a different set of objectives and privacy concerns thus are beyond the scope of this paper. For example, their movements are entirely public, far in advance. Privacy concerns are instead related to passenger or crew information, or potentially commercially sensitive data such as fuel on board or maintenance issues. Since this paper looks at privacy tied to location, we consider commercial aircraft out of scope.

5.1 Business

Business stakeholders typically fly jets capable of 4–20 passengers. Gulfstream's G-range or Bombardier's Learjet and Challenger aircraft are popular choices. There are also business airliners based on commercial airframes produced by Boeing and Airbus, which in their VIP and corporate versions constitute the high-end of the market capable of carrying 100+ passengers. Business flights can either be commercial on-demand services (e.g. aircraft chartering) or, if the aircraft is owned by the operator and used without hire, can be counted under general aviation. They are used to transport personnel to meetings, conferences or other gatherings.

Table 1. Breakdown by stakeholder of identifiable aircraft (AC) using the ACARS data link. We focus on business, military and government aircraft in this work.

Stakeholder type	# Aircraft (% all aircraft)	# ADS-B equipped (% AC category)
Commercial	6916 (69.7%)	6843 (98.9%)
Business	2360 (23.8%)	2316 (98.1%)
Military	442 (4.5%)	427 (96.6%)
Government	200 (2.0%)	193 (96.5%)
Unknown	6 (0.1%)	0 (0.0%)
All	9924 (100%)	9779 (98.5%)

5.2 Military

We classify any aircraft operated by a national air force as military aircraft. Military stakeholders operate in a different way to commercial aircraft. A typically military fleet will consist of some civilian aircraft adapted for military purpose or used for transport, and a set of military-specific aircraft. These aircraft are able to operate in ways civilian aircraft cannot; they can use military-specific communications systems and are permitted to turn off some systems such as ADS-B [23]. Military aircraft types that use ACARS range from modified airliners over business jets to tankers and multi-role transport aircraft, but not fighter jets/combat aircraft.

5.3 Government

Air transport for state officials differs between countries. In some states, the task falls to the flag-carrier airline, in others to the military, and many heads of state own private aircraft. For example in the UK, the Royal Family and government use state-owned, military-operated aircraft [7]. Regardless of the operator, these are often typical business aircraft, from small Gulfstream or Bombardier jets to larger Airbus or Boeing jets for bigger delegations, and tend to operate in similar ways to civilian aircraft.

5.4 Category Statistics

In Table 1 we show the number of aircraft belonging to each stakeholder group described above, along with their level of ADS-B equippage. We assess ADS-B equippage from Opensky Network data, cross-checking ICAO numbers with existence according to Opensky.

Commercial aircraft make up the majority of all ACARS users at 69.7%, with those qualifying as business jets comprising the other significant portion at 23.8%. Military and state-based aircraft were observed to be much smaller at 4.5% and 2.0% respectively—unsurprising considering the exclusivity of these groups. Note the high level of ADS-B equipage across the board; ADS-B poses its own security and privacy challenges and so any system which adds to this compounds the problem further [43, 52].

6 Blocked Aircraft

Many aviation users seek to protect their privacy by obscuring their aircraft movements and communications. In this section, we explore the concept of the 'blocked aircraft' approach to location privacy.

6.1 Background on Aircraft Blocking

By default, aviation movements are publicly visible. This takes many forms; Flightradar24 [18] and FlightAware [16] provide such data for free with the option of paying for API access, whilst the FAA Aircraft Situation Display to Industry (ASDI) offers an industry-quality data feed but requires a contract stipulating how it is used [12]. Some ATC operators share their own data without an API; for example, NATS, the UK ANSP, offers an educational tool called Airspace Explorer [33].

Naturally, some aircraft owners want to restrict the public sharing of their aircraft data. The most established blocking mechanism concerns the FAA data feed: until recently, the National Business Aviation Association (NBAA) ran a programme called Blocked Aircraft Registration Request (BARR) [31]. Submitting a BARR request would allow an aircraft owner to either prevent their data reaching a subscriber (source-level block) or allow it to reach a subscriber but not shared publicly (subscriber-level block). ASDI has been decommissioned but the feed and BARR program are instead part of the new Traffic Flow Management Systems (TFMS). Aircraft owners can submit directly to the FAA for a block, who administrate the list for the new feed. Until recently, the comprehensive list of blocked aircraft was only available to TFMS subscribers and thus private—a Freedom of Information request made a version of this list from March 2017 public [56]. At the time of writing, BARR is the most prominent public blocking scheme with government cooperation. Outside of the US, little evidence of blocking for business aircraft at the national scale exists (though, as identified below, some organized state and military blocking does exist).

For commercial data feeds (or for aircraft registered outside the US) FlightAware provide a fee-paid subscription service through which the owner can block their information from public dissemination [16, 17]. FlightAware explicitly state that they do not track military aircraft, using blocking of US presidential fleet movements as an example. They have also been subject to pressure from military and law enforcement/government aircraft owners [17]. Flightradar24 has limited public information about how to block aircraft but acknowledge that some aircraft display a limited amount, if any, of information on their website [19].

The NATS Airspace Explorer provides an example of collaboration on flight blocking with governmental agencies [33]. The tool does not show a number of sensitive aircraft agreed with the UK Centre for Protection of National Infrastructure (CPNI). Similar statements have been made with regards to the ASDI feed [25].

In each case, we see a clear demonstration that those who are blocked are seeking some level of privacy. As such, we consider that any aircraft using a block has a privacy requirement and ACARS usage which leaks private data is undermining that requirement.

6.2 Motivation for Blocking Aircraft

Table 2 shows a breakdown by aircraft category and the type of block implemented. We claim that efforts to block aircraft from appearing on public data feeds is an effort to obtain some level of privacy—we use this to explain the motivations of the stakeholders. Note that BARR blocks are significantly less frequent than Flightradar24 or FlightAware blocks; this is highly likely to be due to the European collection location, thus observing fewer US-registered aircraft. We include the figures as a reference, due to BARR being a well established governmental scheme.

Table 2. Number of blocked aircraft (AC) from each category observed over each link, and aggregated over all links. FR24 is a Flightradar24 block, FA is a FlightAware block.

Business							
Network	**All AC**	**FR24**		**FA**		**BARR**	
VHF	**1086**	**601**	**55.3%**	**214**	**19.7%**	**118**	**10.9%**
VDL2	**1015**	**930**	**91.6%**	**383**	**37.7%**	**241**	**23.7%**
SATCOM	**970**	**882**	**90.9%**	**426**	**43.9%**	**299**	**30.8%**
All	**2360**	**2145**	**90.9%**	**950**	**40.3%**	**514**	**21.8%**
Military							
Network	**All AC**	**FR24**		**FA**		**BARR**	
VHF	**14**	**13**	**92.9%**	**8**	**57.1%**	**0**	**0.0%**
VDL2	**25**	**19**	**76.0%**	**10**	**40.0%**	**0**	**0.0%**
SATCOM	**418**	**104**	**24.9%**	**88**	**21.1%**	**1**	**0.2%**
All	**442**	**420**	**95.0%**	**368**	**83.3%**	**1**	**0.2%**
Government							
Network	**Total AC**	**FR24**		**FA**		**BARR**	
VHF	**82**	**41**	**50.0%**	**28**	**34.1%**	**12**	**14.6%**
VDL2	**72**	**33**	**45.8%**	**22**	**30.6%**	**8**	**11.1%**
SATCOM	**119**	**66**	**55.5%**	**43**	**36.1%**	**11**	**9.2%**
All	**200**	**108**	**54.0%**	**69**	**34.5%**	**20**	**10.0%**

Business

Blocking business aircraft has been, and currently is, a point of much contention. This is a multifaceted issue which sees shareholders and the public wanting more transparency, whilst companies firmly believe that having no aviation privacy would seriously impede business. Some examples of this are provided in [30], in which blocked aircraft movements are claimed to be able to reveal mergers, acquisitions and personal executive actions which would unduly affect share price.

In [20], a legislative assessment of the BARR program and its history is conducted. The authors favor the existence of such schemes, arguing that whilst the list of those using the BARR program is too general to be harmful, detailed aircraft movements and history as provided by flight trackers indeed has the potential for harm. This provides evidence for the scheme being used as a privacy measure, since the United States Congress have repeatedly enacted it [20]. Outside of the legal precedent, the use of fee-paid schemes to block aircraft suggests that owners are willing to pay to protect their privacy as much as possible [16, 55].

Considering Table 2, we see that around 22% of business aircraft have a BARR block; the lower percentage likely due to our European collection location, thus seeing few US registered aircraft. However, close to 91% have a Flightradar24 block and just over 40% are blocked on FlightAware. The gap between these numbers could be down to the way in which blocks are visible to the user. Flightradar24 shows no information, whereas FlightAware varies in approach; some aircraft show no/old information, some explicitly state they are blocked whereas others apparently do not exist. We only classify the latter two categories as blocked—it appears that many business aircraft take the first approach on FlightAware.

Military & State

Within most of the described blocking mechanisms, military and state aircraft appear to be granted a presumed right to privacy. As highlighted in [20, 33], governments interact with aviation agencies to filter out aircraft before the data is made available to third-parties. This demonstrates a clear desire for operational privacy from both military and state aircraft operators.

Previous research on ACARS security was led by a desire for data privacy from the US Air Force—they wished to use ACARS but were concerned about the fact that all messages were transmitted in the clear [1, 39]. It is worth noting that the government's and military's stance on privacy heavily depends on their stance on transparency. Some countries (e.g., Switzerland) publish military and governmental aircraft records in full [14].

In Table 2 we see that whilst BARR blocks are not common for military or government aircraft, however 95% of military and 54% of government aircraft have blocks on Flightradar24. Furthermore, 83% of military aircraft are blocked on FlightAware. Government aircraft blocking on FlightAware was lower at around 34%. From this we can deduce that blocking aircraft is popular amongst military and government aircraft, implying desire for location privacy. The lack of BARR blocks is likely due to two reasons. Military (and thus government, in the US) aircraft are redacted by default as implied in [25], and since collection occurs in one European location, many aircraft will be of European origin thus not eligible for a BARR block.

Table 3. Transmitting (TX) of positional reports by aircraft (AC) on VHF. Percentages are of all blocked aircraft of that category.

	All AC	Blocked AC	Position Reports	Num. TX AC	Msgs / AC	% Blocked AC
Biz.	1084	976	4828	516	9.40	52.8%
Mil.	14	14	89	5	17.80	35.7%
Gov.	82	46	83	18	4.61	39.1%

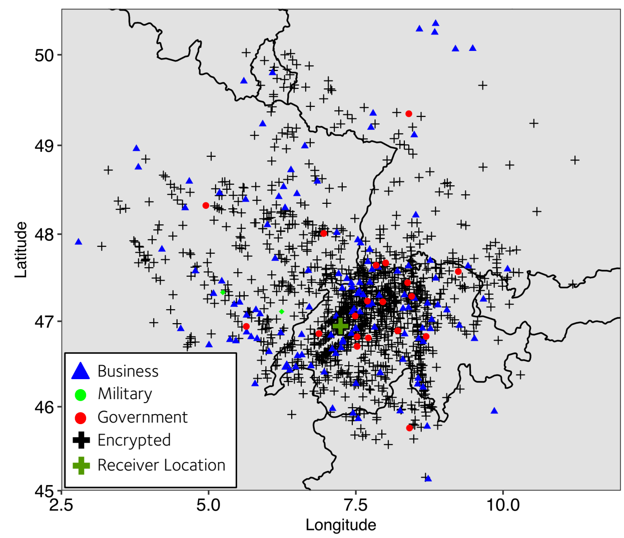

Fig. 2. Plot of both cleartext and encrypted position reports from business, government and military aircraft across all links. Encrypted positional reports are explained in detail in Section 7.3.

7 ACARS and Blocked Aircraft

As outlined above, the vast majority of ACARS messages are sent in the clear, regardless of the originator, and also by aircraft using blocking schemes. During our data collection, we observed 3004 aircraft, 2721 (90.5%) of which were blocked. We now explore the impact of ACARS usage on blocked aircraft and assess the privacy breaches caused by using unsecured communications.

7.1 Position Reporting

One of the many purposes of ACARS includes position reporting. Although ADS-B is slowly becoming compulsory worldwide, ACARS-based position reporting is widely used by business, commercial, military and state aircraft alike. This allows airlines or third-parties to provide services based on location data which they would otherwise not necessarily have access to. Despite the ARINC 620 standard defining some methods to do this, a range of ways to share position are used [4].

Position reporting via ACARS presents a challenge to aircraft which are trying to avoid being detected from transmissions of other systems, such as ADS-B. Because of this, it poses location privacy issues as a result of a lack of cryptographic protection. We look at two types of report: Automatic Dependent Surveillance-Contract (ADS-C) and text-based.

ADS-C. ADS-C is a point-to-point, rather than broadcast, method for surveillance. It establishes a reporting contract with ATC and based on this, feeds position over data link [24]. These messages are encoded but may contain more information than ADS-B messages, including imminent waypoints, notification of route changes and emergency events. Transmitting ADS-C messages on an unprotected link can reveal a lot of routing data; for aircraft which wish to hide this, it becomes a privacy issue.

Blocked aircraft usage of ADS-C was mostly confined to the military on SATCOM, with 104 blocked aircraft (25.7% of all military blocked on SATCOM) sending 1062 messages. As we only observe SATCOM uplink, we can only see the ground-to-air side of ADS-C, e.g. requesting reports. However, one can determine which aircraft use the system, thus reveal their location. An average aircraft sent 10 messages with one US Air Force aircraft receiving 171 messages alone, indicating heavy use of ADS-C on downlink.

Text-Based Position Reports. Whilst ADS-B and ADS-C provide well-defined systems for transmitting location, our data shows that many aircraft send positional reports outside of this. Often, they simply send coordinates as part of a message, along with a timestamp. This is heavily used on the POA link above all others, as illustrated in Table 3, also plotted in Figure 2. In this, we observe a nominal range of 400 km, with three outliers at 430, 440 and 460 km. It saw just over 52% of blocked business, 35% military and 39% government aircraft sending such messages. Furthermore, these aircraft sent 9.4, 17.8 and 4.6 messages each, respectively. The situation for certain business aircraft is somewhat worse on SATCOM; although only 13.9% of blocked aircraft send this type of message, they on average send 12.8 messages each. We look at text-based position reporting further in Section 7.3.

Clearly, this is a significant problem for business aircraft in particular. Any notion of obscuring oneself from a flight tracker is undermined somewhat by sending ACARS position reports. Although VHF-based ACARS might have a similar range to ADS-B, it is yet another clear text transmission of sensitive data for blocked aircraft. For position reports sent via SATCOM the potential interception range is significantly higher.

7.2 Use of Information Services

Information services, such as the Digital-Aerodrome Terminal Information Service (D-ATIS, or simply ATIS), reveal a great deal about aircraft intention. ATIS reports are used by pilots to reduce ATC load [22] and contain information about an airport such as runway condition and activity, weather, Notices to Airmen (NOTAMs) and other safety-related data. Thus, requesting ATIS information is an intention to land at a given airport; revealing an aircraft's destination and approach timing. Table 4 demonstrates that ATIS is used by blocked aircraft across all links. Whilst usage is confined to a small section of the blocked aircraft for each category, the level is consistent across the categories and the aircraft which use it tend to send several messages.

Primarily on SATCOM, we saw 19% of all blocked business aircraft and 20% of blocked military and government aircraft use ATIS. Business and military aircraft sent three messages each on average, whereas government sent over five. Although a normal part of aviation operation—and an important frequency congestion reducer—it allows a listener to determine where the aircraft is landing. Since this is mostly via SATCOM, the listener need not be geographically close. Because of this, it reveals intention information which would otherwise be hard to gather at this scale. Again, this is a problem for those hiding from public flight tracking.

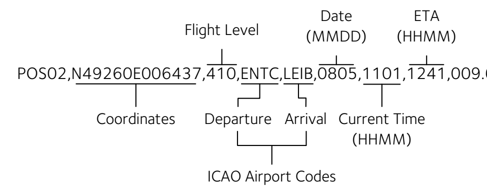

Fig. 3. Labelled plaintext message format of encrypted positional reports, from [48].

7.3 Use of Proprietary Encryption

Proprietary encryption is regularly used by business-type aircraft. In [48] use of a monoalphabetic substitution cipher with hard-coded keys is presented. Our data demonstrates that these messages are sent over all three observed links. Once decrypted, these messages reveal much about the aircraft's route. As indicated in [48], many messages of this type report position. However, unlike Mode-S or ADS-B, they also reveal origin, destination and estimated time of arrival. A labelled plaintext message of this type is in Figure 3. Other messages such as weather reports or free-text transfer of flight plans are encrypted in this way and can reveal the destination airport. In some cases, the latter also reveals previous flight plan by that aircraft via SATCOM.

We observed 166 blocked aircraft (6.4% of all blocked) using this cipher across all links, sending 2783 messages, as shown in Table 4. Whilst a low proportion of blocked aircraft, the few which use it do so heavily. Government aircraft had the lowest average at 9.4 per aircraft, with military at 10 and business at 18.2.

On the POA link, usage was confined to business aircraft. Whilst only 42 (5.1%) blocked aircraft used encrypted messages an average of 21 messages per aircraft were sent. Although the number of users is low,the ones who do use it are at significant leakage risk. On SATCOM the proportion of aircraft using this is a slightly higher at 13.9%, who on average send 12.8 messages each. This link also sees the highest level of military and government usage; whilst only 6 aircraft each, they both sent 10 messages on average.

Of the encrypted messages, 33.5% were positional reports of which 96.9% originated from blocked aircraft. These aircraft otherwise obscure their actions, and use a cipher to further obscure the data. The fact that these messages are trivial to decrypt and contain aircraft intention information constitutes a clear privacy issue.

Table 4. Extent of business, military and government aircraft (AC) using messages encrypted with a proprietary cipher, and ATIS requests/responses. Data is aggregated across all three links.

	All Aircraft	Blocked Aircraft	Encrypted Messages	# AC Sending	Avg. per AC	% Blocked Aircraft	ATIS Messages	# AC Sending	Avg. per AC	% Blocked Aircraft
Business	2360	2170	2657	153	17.4	7.1%	1210	322	3.8	14.8%
Military	442	424	60	6	10.0	1.4%	314	84	3.7	19.8%
Gov't	200	127	66	7	9.4	5.5%	115	22	5.2	17.3%

Many further message types exist, including weather reports for airports, flight plan recalling and a basic email system. Each can leak information about aircraft activity but the level of sensitivity is low. Weather reports for airports can be used to check the conditions on approach, however usage is inconsistent unlike ATIS. Meteorological reporting comprised 43.2% of the encrypted messages, with 93.5% coming from blocked aircraft. The remaining 23.7% of messages were either unrecoverable or free text messages.

7.4 Flight Plans

SATCOM transmission of flight plans is used by 69% of blocked military aircraft; since 405 of the 418 military aircraft on the link are blocked, the majority of this group of aircraft engage in this. The average observed aircraft sent around four messages. Depending on the country of origin, the format of these messages varies.

Typically, the message content is used to transfer flight plan data to the aircraft. Similar to clearances, this involves the departure and arrival airports and in some cases routes and call signs. Call signs can indicate the type of flight—for example, "RCH" is a 'reach' flight, which is a troop transport. Since military aircraft have a degree of operational sensitivity, the fact that these messages are sent in clear text at all is a problem. Additionally, a significant proportion of these aircraft have both a Flightradar24 and FlightAware block in place, indicating that there is some active, rather than just presumed, attempt at privacy. We look at military usage of flight plans further in Sec. 8.2.

Although not directly related, some military aircraft on SATCOM make use of free text messages on a similar protocol. We observed 115 blocked military aircraft sending 630 messages in this way. Most of these include flight operational content relating to cargo or estimated arrival times, with some revealing destinations or route adjustments.

7.5 Undermining Aircraft Blocks

Clearly, use of ACARS by business, military and state aircraft poses a significant threat to privacy. By listening to the ACARS mediums in a single location, messages worldwide can be collected and used to track movements and reveal intentions. Although some aircraft might not consider this a problem, a significant proportion of blocked aircraft (of which 90.5% of the non-commercial aircraft observed were) use clear text messages—or an easily breakable cipher—to transfer information which they otherwise try to obscure from public knowledge.

It is important to compare data obtained from ACARS with similar data gathered by collecting airport landing logs or listening to ATC voice channels. In order to gather data from landing logs or flight plans, copies must be acquired from ANSPs and then processed. To cover numerous countries would incur a lot of manual work; on top of this, some countries or airports may not make all of their logs public. ACARS provides more structured, consistent data stream than this—having a formal message structure makes it easier to process at scale. Furthermore, the structure is the same worldwide, meaning low-cost sensors could be geographically distributed in order to significantly scale up collection.

For ATC communications, language processing could be used as shown in [21], with multiple receivers tuned to different frequencies. This can provide granular information including turn headings and airspeeds of aircraft. However, aircraft regularly change frequency as they move between different areas, thus adding regular risk of losing tracking. On top of this, voice channel quality is variable and congested, so not all phrases can be recovered. Although ACARS may provide less detail, it avoids these challenges. It also offers operational information which would not appear on ATC voice channels.

For these reasons, we feel that ACARS usage by blocked aircraft poses an additional and unique risk to said aircraft privacy beyond the accepted (or known) risk.

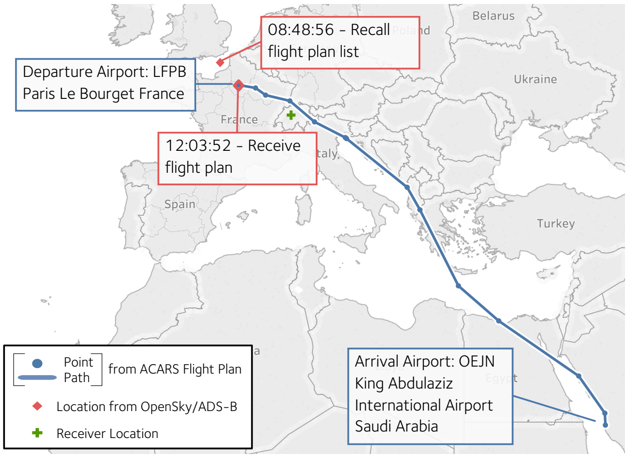

Fig. 4. Flight plan of a blocked business aircraft from SATCOM ACARS messages. Red shapes indicate position obtained from OpenSky ADS-B. Pink/black shapes constructed from flight plan.

8 Case Studies

With the various ways in which ACARS usage can cause problems explained, we now present three case studies to expand upon this. For each aircraft category we show how sending one or more of the message types above can reveal a significant information about a flight; in each case, this is far more than ADS-B alone, and would be collectable with manual means.

8.1 Business Aircraft Case Study

Many business aircraft reveal their locations or destinations with positional reports. However, some cases reveal even more through flight plans and ATIS reports. In this case study, we look at a business jet owned by a Saudi Arabian company and operated by a British private aviation firm. This aircraft regularly transmits on SATCOM, sending 118 messages of which 50 were encrypted with a monoalphabetic cipher, 10 were ATIS and 10 were flight plans. This aircraft has a BARR source block and is blocked on both web trackers.

In Figure 4 we see the reconstruction of one day of ACARS traffic, consisting of 20 messages. This data is cross-referenced with OpenSky, a collaborative sensor network collecting ADS-B and Mode S data for use by researchers [44]. Seemingly whilst flying to the departure airport, it is sent the list of available flight plans, then whilst on approach, is sent the flight plan for the flight Paris to Jeddah. Using the flight plan we can construct the main waypoints along the flight. It follows this message with some considerably more detailed route information over the course of three messages. Two hours later, the aircraft resumes sending messages, though this time no ADS-B data could be retrieved. During this period it sends 10 encrypted messages and uses ATIS to check the landing conditions at the arrival airport.

Clearly, this is a significant amount of information recovered from relatively few messages, especially for a blocked aircraft. A similar process could be followed for the other flight plans and exchanges; when considering the fact that the aircraft is apparently blocked on all public flight trackers, this is a significant leak.

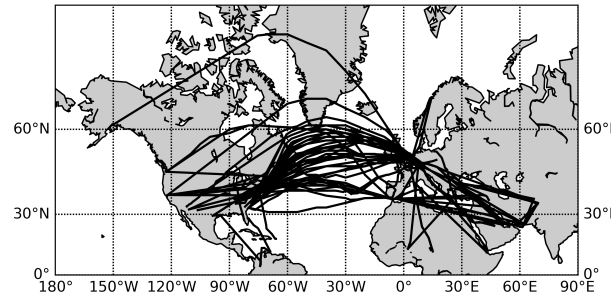

Fig. 5. Plotted flight tracks from flight plans received by blocked military aircraft over the SATCOM data link.

8.2 Military Aircraft Case Study

Military aircraft are permitted to turn ADS-B off in order to provide privacy with respect to their location [23]. As shown in Table 4, 424 (95.9%) of these aircraft were using some kind of block on flight tracking websites. We can see there is a real desire for privacy, as many of these aircraft were ‘unknown’ to the trackers.

These aircraft made much use of ACARS, with the average aircraft sending three messages in the collection range. Some reveal much more than others, however. Over our collection phase we received over 1206 flight plans transmitted by 280 blocked military aircraft via SATCOM. We were able to reconstruct the flight path for most of them, as shown in Figure 5.

We present the case of a specific military aircraft to demonstrate the impact of ACARS further. An American military aircraft observed solely over SATCOM transmitted 513 messages between November 2016 and January 2017. Message content varied between free text, flight plans and weather reports.

When looking specifically at the of this aircraft flight plans we can see a lot of aircraft; despite being blocked it received 16 flight plan and 32 ATIS messages. On top of this, it transmitted messages providing far more detailed routes, apparently updates on the route taken so far. In one instance the aircraft transmitted a flight plan, then an update 40 minutes later. We have

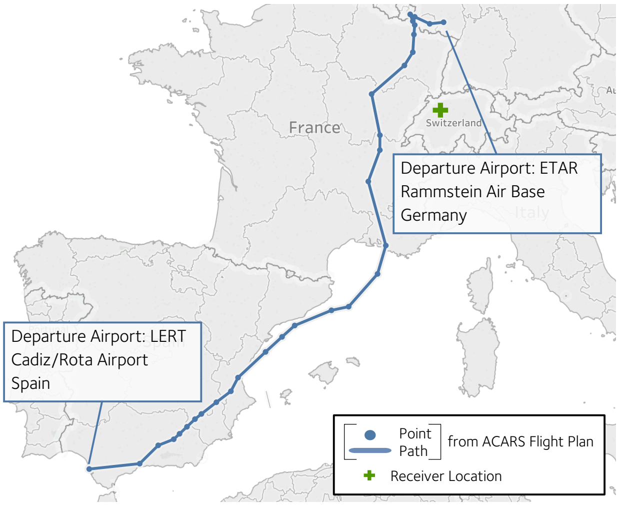

Fig. 6. Plotted flight update from a US military aircraft in January 2017. This was collected on the SATCOM link.

plotted this update in Figure 6. Despite the aircraft being blocked on flight tracking websites, an attacker can plot the movements of this aircraft based on either of these messages, collected far away from the departure airport. Importantly, by using both the flight plan and update, they can see where the aircraft is going without relying on more regular updated information.

8.3 State Aircraft Case Study

An example of the power of these messages is in messages collected from an aircraft of the US diplomatic fleet. This particular aircraft appeared to have a source-level block, since it is considered US military. As such, no information about it can be seen in FlightRadar24 or FlightAware at the time of collection. Using both POA and SATCOM ACARS, we were able to not only receive messages and track the aircraft as it flew over our collection location, but also were able to gather loadsheets and a flight plan. Figure 7 shows that five SATCOM ACARS messages collected within an hour reveal the full route, despite the collection location being in middle of the route. These messages were received before the aircraft entered VHF range, out of the line of sight.

Using Mode S and ADS-B data from OpenSky, we see the additional level of sensitive positional data leaked by ACARS. Firstly, the aircraft rarely turns ADS-B on apart from a period of 27 minutes at cruise altitude over France. This appears to be some attempt at hiding, since ADS-B is mandated for use by all civilian aircraft in US and European airspace by 2020 [13]—military aircraft do have the ability and permission to turn this off though [9, 23]. Alongside the flight plans revealing the origin, destination and waypoints along the route, other messages include an loadsheet for items on-board. In terms of the latter, most is standard information, e.g. passenger count, fuel and take-off parameters. This has potential sensitivity since it indicates how many passengers are on board and as such, the type of mission underway. However, additional items are seemingly coded entries such as 'WHITE ELEFANT', 'GREY GHOST'. No public information on these items exist yet they appear in a number of loadsheets sent by US diplomatic fleet aircraft.

Beyond this flight, the aircraft conducted other flights revealing route information, ADS-C updates, further inventories and free-text messages.

9 Industry Opinions

ACARS is used by many stakeholders within aviation, each interacting with it in different ways. Our survey aimed to understand privacy—and relevant security—perceptions of ACARS. Whilst we have contextualized some parts of the paper already with results from the survey, we now look specifically at industry professional views on ACARS usage for sensitive data. We surveyed 40 aviation professionals, including pilots, avionics engineers and air traffic controllers.

In order to understand the general level of awareness of sensitive data being sent over ACARS, part of the survey asked the following three questions:

1. Do you have any experience of ACARS being used to share sensitive or private information? This might include personal data (e.g. names, addresses) or commercially sensitive data.
2. How suitable would you consider standard ACARS (unencrypted) to be from a privacy point-of-view? For example, for transmitting sensitive data such as names or addresses.
3. How suitable would you consider standard ACARS (unencrypted) to be from a safety point-of-view? In other words, to what extent do you think that ACARS is secure enough for safety-related data?

Since we know that ACARS does not offer security by default, these questions aimed to understand whether such a lack of security has an impact on the perception and usage of ACARS. In the first question we simply try to understand whether those surveyed had experienced a form of the problem described in this paper. Figure 8 displays the results, and indicates that whilst most did, the response was somewhat mixed. This could indicate

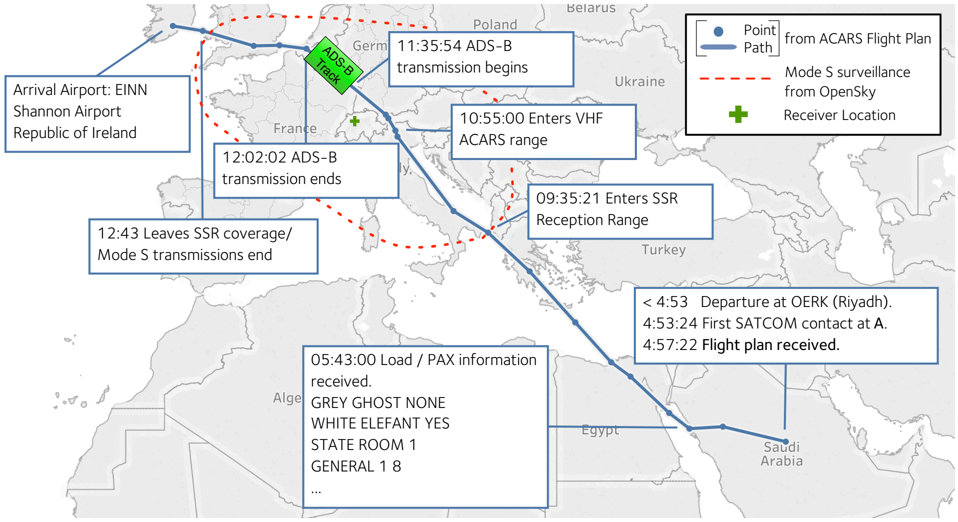

Fig. 7. Flight track of a US Diplomatic fleet aircraft in December 2016, reconstructed from ACARS messages. Note that aircraft switches on ADS-B only for cruising, never for departure or landing.

differing views on what constitutes private data, but equally highlights how much wider of a system view that the attacker described in this paper would have. In the context of the work surrounding ACARS privacy, it is clear that there is a debate amongst the aviation community about which data needs to be secured.

Our second question relates to the results of this paper; i.e. that aircraft operators are unknowingly leaking sensitive location data over ACARS, and the privacy implications of this. Results are shown in Figure 9, with 31 of those responding (77.5%) feeling that ACARS is either 'somewhat unsuitable' or 'very unsuitable' for such data. Indeed, this matches with our findings and is promising with regards to addressing the problem.

The third question, relating to safety, provides a comparison point to Q2 i.e., if users consider ACARS unsuitable for private data whether they also consider it unsafe. Intuitively, if ACARS lacks security measures (namely integrity and authentication protection), then its ability to provide safe communication would be compromised. As shown in Figure 9, 17 respondents (42.5%) did not agree with this view, which given the focus on safety in aviation is noteworthy. It can be seen that the bias is towards ACARS being 'unsuitable' for privacy, but towards 'suitable' for safety. We believe that this difference is a cause for concern should ACARS be used for safety-critical data in the future.

Clearly, ACARS is considered to be a reasonable system in the aviation industry for some purposes; indeed, this is expected given the level of deployment and usage. Despite experiences of private data over ACARS being mixed, it is clear that there is an understanding

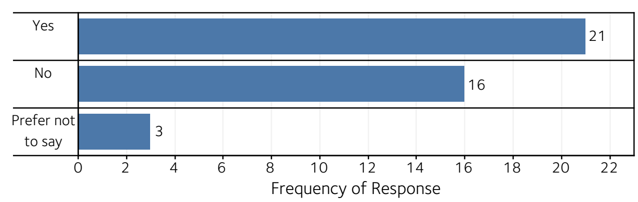

Fig. 8. Chart for Question 1, "Do you have any experience of ACARS being used to share sensitive or private information? "

of the privacy issues on ACARS. However, this does not match up with practice; indicated awareness has not yet caused changes in the way the link is used. One reason could be that air traffic controllers or pilots do not have a choice of which system to use—ACARS is simply all they have. Another likely cause is that there is a disconnect between the owners, pilots, controllers and engineers who understand the desire for privacy and those who do not. Not having a consensus on security and privacy creates the issues described in this paper.

10 Mitigations

Many of the leaks described in Section 7 are as a result of the message content; without it, the most a single receiver can determine is the aircraft existence. Because of this, protecting message content is paramount. We cover two types of approach to this: technical and policy.

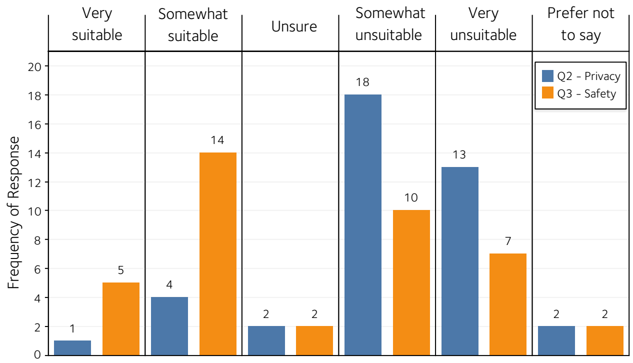

Fig. 9. Charts for Question 2, "How suitable would you consider standard ACARS (unencrypted) to be from a privacy point-of-view?" and Question 3, "How suitable would you consider standard ACARS (unencrypted) to be from a safety point-of-view?"

10.1 Technical Measures

There are some existing technical measures (in practical use or standardized) by which ACARS message content can be protected. However, whilst they can provide improved security, they also have noteworthy drawbacks.

ACARS Message Security

Although ACARS has no security by default, some solutions of varying complexity and effectiveness have been developed as optional 'add-ons'. The most comprehensive systems are based on the ARINC 823P1 standard ACARS Message Security (AMS) [2]. The only existing implementations based on AMS is Secure ACARS [40], which provides message confidentiality and authentication but comes at a surcharge to the ACARS service.

Secure ACARS uses the US National Security Agency's Commercial National Security Algorithm (CSNA) Suite though with older Suite B parameters [32]. However, formal analysis of the ARINC 823 has indicated some weaknesses, thus the standard would need further work to provide modern security [6]. Whilst no official usage figures are public, we have not observed consistent usage of AMS on either SATCOM or VHF channels. Only two (5%) of professionals surveyed had any knowledge of AMS usage in practice, with 36 (90%) having no knowledge of deployment.

Using AMS would likely solve the issue of leaks to a passive attacker, and would do so using standardized cryptographic approaches. It does, however, come with some challenges. As with any distributed security solution, implementing a public-key infrastructure is costly and requires thoughtful, security-conscious design. Especially in the case of aircraft, which must be able to communicate with unexpected ground stations, keeping up-to-date credentials for all communication partners is a key challenge. Furthermore, it requires specific software and hardware updates, which take a lot of time and money to produce and deploy. Already, the cost of Secure ACARS has proven to be a major hindrance and the main reason for its almost non-existent deployment, even though the investment may be offset by the potential reputational damage and legal costs.

Non-standardized Cryptography

In lieu of the standardized AMS, non-standardized and potentially proprietary cryptography is used by some operators (see Section 7.3). Naturally, the effectiveness of such measures depends entirely on the quality of the cryptography. Thus far, all attempts at this that we have been able to identify in the wild have provided no meaningful level of security but rely on insecure monoalphabetic substitution ciphers instead.

While the temptation of such cheap, proprietary cryptographic solutions is great (as observed in wide use, for example on business jets [48]), weak encryption is to be avoided at all costs. Providing the illusion of security and no more, this approach detracts from the importance of quickly deploying well-developed solutions to aircraft. As part of our survey of industry professionals, 5 (12.5%) knew of proprietary encryption use in practice, with 32 (80%) having no knowledge of such a system. This indicates current deployment is limited—but when compared to our data, it can be seen that many business aircraft use it.

This is not to dismiss non-AMS cryptography out-of-hand. It could be deployed faster than standardized efforts and still designed within the restrictions of ACARS. To be effective it must be thoroughly tested by cryptography experts. However, as key management is still likely to be an issue, this solution is best used within a company or organisation rather than being a general solution. Even so, it might still require some change to hardware but if implemented as an ACARS peripheral, would be easier to deploy.

Disabling ACARS Messages

As ACARS is not a technology mandated by any civil aviation authorities, it is legally feasible to forgo its use partly or completely. Some commercial airlines such as Ryanair do not use ACARS, reportedly due to cost reasons, and rely instead on mobile phone networks while they are close to the ground [26]. Thus, it is theoretically conceivable though operationally complicated and costly to abstain from using ACARS for most aircraft.

Instead of this extreme option, a monitoring system could be deployed at the network level to identify only potentially privacy-sensitive messages. Aircraft which wish to partake in this could request that certain message types be blocked from transmission if they are sent unencrypted. Since business, military and government aircraft which wish to hide from public data sources already make an effort to do so, they could register a set of ACARS message restrictions for their aircraft. This way, should those messages be sent without their knowledge, they would be filtered at the network level.

Of course, this would still restrict functionality for some of the aircraft and their operators. It would not work for ATC clearances, for example, which would cause the flight crew to have to fall back to voice communications. However, in the case of blocked aircraft transmitting position reports, many are using ADS-B thus have that as a source of tracking. Since ACARS is not designed for tracking it is arguably better—unless there is a specific reason otherwise—to use ADS-B which is designed for the purpose. Indeed, it would be one fewer privacy risk to defend against.

10.2 Policy Measures

Another option lies in the creation of better policies to improve data security over ACARS. Of course, these are not mutually exclusive to technical measures, but may be more feasible to deploy in a timely fashion considering the often decade-long development cycles found in aviation [51]. As analyzed in the previous sections, unless an effective security measure is in place none of the data links should be used to transfer sensitive data. A strong sensitive data policy could stem the issues described in this paper without heavily reducing functionality.

Data Protection Laws and Regulations

In many parts of the world, data protection legislation is a key measure in enabling citizens to protect their privacy. This is particularly relevant to the aviation scenario; those on board the aircraft are unlikely to control how their data is treated, and the primary method of transferring data is by default not secured.

As an example, the current European Union (EU) data protection regulation was introduced in 1995 [10]. Section 8, Article 17 mandates the security of data processing. Specifically, the data controller must ensure "appropriate technical and organizational" measures are taken to protect against loss, accidental disclosure and modification. Instances of sensitive data transmission over standard ACARS are an obvious breach of this regulation. This regulation will become more powerful soon as new legislation increases fines to the greater of 4% of company turnover or €20 million [11].

Regulations are also relevant to business charter jets, where insecure transmission of private data can violate data protection rules. The clear-text nature of ACARS makes it easy to detect and prove the mishandling of sensitive data, posing a serious litigation risk.

Internal Procedures and Education Policies

While regulations and legislation from governments or aviation authorities can provide compensation to affected entities, this approach is not a quick fix. Although in the medium term it lead to the adoption of existing technical measures or the development of new ones, this would rely on the harshness of the regulations. Thus, in the short term, it is crucial to educate users both on the ground an in the air on the fact that all communication sent via ACARS is effectively public and should be treated as such. Our survey indicates that this is not currently the case. Where possible, codified processes should be adapted to reflect this mindset. While this is not offering a complete solution to the security issues of ACARS, it can at least mitigate them.

An example for how such policies can be effective was provided during our measurement campaign conducted for this paper. As has been reported previously, some air transport providers use ACARS to validate credit cards used for substantial purchases on board of aircraft [47]. We notified several airlines of their misuse of ACARS and provided proof of intercepted data. Until the time of submission, at least one airline responded to us and changed their procedures to close this particular data protection issue by using tokens instead.

10.3 Future Steps

In the longer term, steps should be taken to move away from the current ACARS technology completely, or at least to data links with network-level security. Since it was designed with a significantly weaker threat model in mind—i.e. one of no malicious activity—it is not equipped to deal with cybersecurity threats. As discussed, uptake on available security solutions has been limited, which indicates that a newly developed data link with security as the default, may be the better option. However, given typical technological cycles in aviation, this would take decades to deploy fully [51].

In the meantime, our recommendation is that aircraft which insist on using ACARS fully but require security seek out AMS or similar system; these systems do exist, but simply cost more. Where possible, duplication of systems (e.g. position reporting with ADS-B) should be stopped such that sensitive data is not sent in the clear on two channels. Beyond this, the fastest way to achieve change in ACARS security and privacy will be to educate users such that they demand better systems.

11 Related Work

Nearly a decade before avionics communication gained interest in the scientific community, the United States Air Force published concerns about the security and privacy of ACARS [39]. To keep military frequencies clear for tactical communication, they propose an encryption and authentication system to allow military aircraft to communication over commercial data link.

Since this, work has highlighted the privacy and security issues of ACARS. Most recently, [46] presented some anecdotal evidence for these issues indeed motivating the more comprehensive approach taken in this paper. In [49], the impact of ACARS being transmitted in the clear is discussed specifically with respect to the level of trust which can be placed in the link, though without further quantification. Outside of the academic community, ACARS has received some attention at hacking conferences due to its lack of integrity and authentication mechanisms [54].

A survey in the avionics community was conducted in [50] to find how the actual users assess the security and trustworthiness of the avionics protocols. Most responders believed the likelihood of attacks to be low and trustworthiness was rated above average for most protocols, including ACARS.

Privacy properties of the avionic surveillance system ADS-B are investigated in [41, 42]. Since a passive attacker can trivially receive ADS-B messages, they investigate the effectiveness of the standardized privacy approach—identifier randomisation. They show that knowledge of one identifier allows calculation of subsequent identifiers for the same aircraft; to mitigate this they propose decorrelated random identifiers. More recently, [52] has shown that by collecting ADS-B messages from a region over a long period of time can reveal government- and business-sensitive actions such as meetings, mergers and acquisitions.

Transport privacy is not a purely aviation focussed problem and does not restrict itself to public transport either. In [38], the authors investigate the privacy and security of current car sensor systems focussing on tire pressure systems. An attacker is able to read the static identifiers of the tire pressure sensors from tens of meters away thus allowing tracking of individual vehicles crossing the an attacker checkpoint. Exploting in-car networks [27], discusses how an attacker can use the CAN bus to extract data from the vehicle. Indeed, most of these systems lack even basic security features.

12 Conclusion

In this paper we demonstrate that ACARS usage poses a notable privacy risk to business, military and government across all three data links. Basing privacy on the notion of blocking aircraft and the legal, political and governmental pressures relating to it, we showed that for a modest attacker with a single set of sensors, much can be learned. This is particularly true of the SATCOM link which can collect far beyond line-of-sight to the aircraft due to the nature of the link. With further investment, an attacker could—for a relatively low cost—expand collection to a significant area and capture a great deal of privacy sensitive data.

After highlighting the message types which cause the most significant location privacy issues we illustrate the problem with case studies. This emphasises the importance of ACARS privacy for the military and government stakeholders, as both revealed a lot of data that they otherwise try to conceal. We contextualized this with industry opinions, showing that there is little awareness of existing security in ACARS, even if those surveyed believe that it is not suitable for private data. We concluded by providing mitigations and recommendations, given that this is not a patchable problem—ultimately highlighting the fact that aviation must account for security at the point of design in the future.

Acknowledgements

This work has been supported by the Engineering and Physical Sciences Research Council UK (EPSRC UK), as part of the Centre for Doctoral Training for Cyber Security at the University of Oxford; it has also been supported by the Zurich Information Security and Privacy Center. It represents the views of the authors.

References

[1] C. Adams. Securing ACARS: Data Link in the Post 9/11 Environment. *Avionics Magazine*, pages 24–26, June 2006.

[2] Aeronautical Radio Inc. (ARINC). DataLink Security, Part 1 - ACARS Message Security. Technical Standard 823P1, 2007.

[3] Aeronautical Radio Inc. (ARINC). Aircraft Communications Addressing and Reporting Systems (ACARS). Technical Standard 724B-6, 2012.

[4] Aeronautical Radio Inc. (ARINC). Datalink Ground System Standard and Interface Specification. Technical Standard 620-8, 2014.

[5] Airline Pilots Association. Aviation Cyber Security: The Pilot's Perspective. Technical report, Air Line Pilots Association Int'l, Washington, 2017. URL https://www.rtca.org/sites/default/files/symposium_2017_cybersecurity_white_paper_digital.pdf.

[6] B. Blanchet. Symbolic and Computational Mechanized Verification of the ARINC823 Avionic Protocols. In *2017 IEEE 30th Computer Security Foundations Symposium (CSF)*, pages 68–82, Aug 2017. 10.1109/CSF.2017.7.

[7] J. Bourn. Royal Travel by Air and Rail. Technical report, United Kingdom National Audit Office, London, 2001. URL https://www.nao.org.uk/wp-content/uploads/2001/06/010225.pdf. Retrieved on 2017-01-18.

[8] J. Drew. Managing Cybersecurity Risks, 2012. ISSN 00218448.

[9] Eurocontrol. Aircraft Equipage Requirements in the European Commission IRs 1207/2011 and 1028/2014, 2017. URL https://www.eurocontrol.int/spi-ir.

[10] European Parliament. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995.

[11] 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/EC (General Data Protection Regulation), 2016.

[12] Federal Aviation Administration. Access to Aircraft Situation Display (ASDI) and National Airspace System Status Information (NASSI), 2011. URL https://www.federalregister.gov/documents/2011/03/04/2011-4955/access-to-aircraft-situation-display-asdi-and-national-airspace-system-status-information-nassi. Retrieved on 2017-01-22.

[13] Federal Aviation Administration. Equip ADS-B, 2016. URL https://www.faa.gov/nextgen/equipadsb/. Retrieved on 2016-07-25.

[14] Federal Office of Civil Aviation FOCA. Swiss Aircraft Registry, 2017. URL https://www.bazl.admin.ch/bazl/en/home/specialists/aircraft/swiss-aircraft-registry.html. Retrieved on 2017-02-28.

[15] FlightAware. FlightAware, 2017. URL https://www.flightaware.com/. Retrieved on 2017-03-06.

[16] FlightAware. Global Flight Tracking, 2017. URL http://uk.flightaware.com/commercial/global. Retrieved on 2017-10-19.

[17] FlightAware. Frequently Asked Questions, 2018. URL https://uk.flightaware.com/about/faq#military.

[18] Flightradar24 AB. Flightradar24, 2017. URL https://www.flightradar24.com. Retrieved on 2017-10-06.

[19] Flightradar24 AB. Flightradar24 FAQs, 2018. URL https://www.flightradar24.com/faq. Retrieved on 2018-03-15.

[20] O. Gurtovaya. Maintaining Privacy in a World of Technological Transparency: The BARR Program's ups and downs in Changing Times. *Journal of Air Law and Commerce*, 77: 569–603, 2012.

[21] D. Hoffman and S. Rezchikov. Busting the BARR: Tracking "Untrackable" Private Aircraft for Fun & Profit. In *DEF CON 20*, Las Vegas, 2012. URL https://www.defcon.org/html/defcon-20/dc-20-speakers.html#DHoffman.

[22] International Civil Aviation Organization. Data link-automatic Terminal Information Service (D-ATIS). In *Annex 11 to the Convention on International Civil Aviation - Air Traffic Services*, chapter 4, pages 4–4. 13th edition, 2001.

[23] International Civil Aviation Organization. Guidance Material on Advice to Military Authorities Regarding ADS-B Data Sharing, Sept. 2012.

[24] International Civil Aviation Organization. Automatic Dependent Survey - Contract (ADS-C). In *Global Operational Data Link Document (GOLD)*, chapter 2, pages 2–46. 2nd edition, 2013.

[25] N. B. Kalinowski. Access to Aircraft Situation Display to Industry (ASDI) and National Airspace System Status Information (NASSI) Data., 2012. ISSN 00976326. URL http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=75291461&site=ehost-live.

[26] M. Kirby. How Ryanair monitors health of Boeing 737s without ACARS, 2014. URL https://runwaygirlnetwork.com/2014/09/06/how-ryanair-monitors-health-of-boeing-737s-without-acars/. Retrieved on 2017-11-29.

[27] P. Kleberger, T. Olovsson, and E. Jonsson. Security Aspects of the In-vehicle Network in the Connected Car. In *Intelligent Vehicles Symposium (IV), 2011 IEEE*, pages 528–533, June 2011.

[28] R. D. Kloth. Airframes.org, 2016. URL http://www.airframes.org/. Retrieved on 2017-02-14.

[29] T. Leconte. ACARSDec ACARS Decoder, 2015. URL http://sourceforge.net/projects/acarsdec/. Retrieved on 2016-12-08.

[30] M. Maremont and T. McGinty. FAA Is Set to Give Investors a Peek at M&A Air, 2011. URL https://www.wsj.com/articles/SB10001424052702303499204576389923856575528.

[31] National Business Aviation Administration. Blocking display of Aircraft Situation Display to Industry (ASDI) data, 2016. URL https://www.nbaa.org/ops/security/asdi/.

[32] National Security Agency. Commercial National Security Algorithm (CSNA) Suite, 2015. URL https://www.iad.gov/iad/library/ia-guidance/ia-solutions-for-classified/algorithm-guidance/commercial-national-security-algorithm-suite-factsheet.cfm. Retrieved on 2017-02-21.

[33] NATS. Airspace Explorer FAQs, 2017. URL https://www.nats.aero/ae-home/faqs/. Retrieved on 2017-11-24.

[34] R. T. Oishi and A. Heinke. Data Communications. In C. R. Spitzer, U. Ferrell, and T. Ferrell, editors, *Digital Avionics Handbook*, chapter 2, pages 2.7 – 2.13. CRC Press, 3rd

edition, 2015.

[35] R. T. Oishi and A. Heinke. Air-Ground Communication. In C. R. Spitzer, U. Ferrell, and T. Ferrell, editors, *Digital Avionics Handbook*, pages 2.1 – 2.3. Taylor & Francis Group, third edition, 2015.

[36] J. Olds. JAERO, 2017. URL https://github.com/jontio/JAERO. Retrieved on 2017-05-08.

[37] K. Pascoe. ACARS and Error Checking, 2015. URL http://www.flight.org/acars-and-error-checking. Retrieved on 2017-11-07.

[38] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar. Security and Privacy Vulnerabilities of In-car Wireless Networks: A Tire Pressure Monitoring System Case Study. In *Proceedings of the 19th USENIX Conference on Security*, USENIX Security '10, pages 21–21, Berkeley, CA, USA, 2010. USENIX Association.

[39] A. Roy. Security Strategy for US Air Force to Use Commercial Data Link. In *19th Digital Avionics Systems Converence*, pages 1–8, Philadephia, 2000. IEEE Computer Society. ISBN 0780363957.

[40] A. Roy. Secure Aircraft Communications Addressing and Reporting System (ACARS). US Patent 6677888, 2004.

[41] K. Sampigethaya and R. Poovendran. Flight Privacy in the NextGen: Challenges and Opportunities. In *Integrated Communications, Navigation and Surveillance Conference (ICNS), 2013*, pages 1–15, Apr. 2013.

[42] K. Sampigethaya, R. Poovendran, S. Shetty, T. Davis, and C. Royalty. Future E-enabled Aircraft Communications and Security: The Next 20 Years and Beyond. *Proceedings of the IEEE*, 99(11):2040–2055, 2011.

[43] M. Schäfer, V. Lenders, and I. Martinovic. Experimental Analysis of Attacks on Next Generation Air Traffic Communication. *Lecture Notes in Computer Science*, 7954 LNCS: 253–271, 2013. ISSN 03029743. 10.1007/978-3-642-38980-1_16. URL http://link.springer.com/chapter/10.1007/978-3-642-38980-1_16.

[44] M. Schäfer, M. Strohmeier, V. Lenders, I. Martinovic, and M. Wilhelm. Bringing Up OpenSky: A Large-scale ADS-B Sensor Network for Research. *IPSN 2014 - Proceedings of the 13th International Symposium on Information Processing in Sensor Networks (Part of CPS Week)*, pages 83–94, 2014.

[45] M. Schäfer, M. Strohmeier, M. Smith, M. Fuchs, R. Pinheiro, V. Lenders, and I. Martinovic. OpenSky's Report 2016: Facts, Figures and Trends in Wireless ATC Communication Systems. In *35th Digital Avionics Systems Conference - Proceedings*. IEEE/AIAA, 2016.

[46] M. Smith, M. Strohmeier, V. Lenders, and I. Martinovic. On the Security and Privacy of ACARS. In *Integrated Communications Navigation and Surveillance Conference (ICNS)*, Herndon, 2016.

[47] M. Smith, D. Moser, M. Strohmeier, V. Lenders, and I. Martinovic. Analyzing Privacy Breaches in the Aircraft Communications Addressing and Reporting System (ACARS). *ArXiv e-prints*, May 2017. URL https://arxiv.org/pdf/1705.07065.pdf.

[48] M. Smith, D. Moser, M. Strohmeier, V. Lenders, and I. Martinovic. Economy Class Crypto: Exploring Weak Cipher Usage in Avionic Communications via ACARS. In *21st International Conference on Financial Cryptography and Data Security*, Malta, 2017.

[49] P. E. Storck. Benefits of Commercial Data Link Security. In *Integrated Communications, Navigation and Surveillance Conference, ICNS*, Herndon, 2013. IEEE.

[50] M. Strohmeier, M. Schäfer, R. Pinheiro, V. Lenders, and I. Martinovic. On Perception and Reality in Wireless Air Traffic Communications Security. 2016. URL http://arxiv.org/abs/1602.08777. Retrieved on 2016-10-05.

[51] M. Strohmeier, M. Smith, M. Schäfer, V. Lenders, and I. Martinovic. Assessing the Impact of Aviation Security on Cyber Power. In *Cyber Conflict (CYCON), 8th International Conference on*. IEEE, 2016.

[52] M. Strohmeier, M. Smith, V. Lenders, and I. Martinovic. The Real First Class? Inferring Confidential Corporate Mergers and Government Relations from Air Traffic Communication. In *IEEE European Symposium on Security and Privacy (EuroS&P) 2018*. IEEE, Apr. 2018.

[53] J. Sun. World Aircraft Database, 2016. URL http://junzisun.com/adb/. Retrieved on 2016-11-05.

[54] H. Teso. Aicraft Hacking: Practical Aero Series. In *4th Hack in the Box Security Conference in Europe*, Amsterdam, April 2013. URL https://conference.hitb.org/hitbsecconf2013ams/materials/D1T1-HugoTeso-AircraftHacking-PracticalAeroSeries.pdf. Retrieved on 2017-01-13.

[55] C. Trautvetter. FltPlan Flight Privacy Program Exposes Tangled FAA Policy, 2011. URL https://www.ainonline.com/aviation-news/aviation-international-news/2011-08-31/fltplan-flight-privacy-program-exposes-tangled-faa-policy. Retrieved on 2017-10-24.

[56] T. Webster. FAA: List of Blocked Aircraft (BARR List/ASDI Block List), 2017. URL https://www.muckrock.com/foi/united-states-of-america-10/faa-list-of-blocked-aircraft-barr-listasdi-block-list-34713/. Retrieved on 2017-10-27.

[57] J. Wolper. Security Risks of Laptops in Airline Cockpits, 1998. URL http://catless.ncl.ac.uk/Risks/20/12#subj4. Retrieved on 2017-02-17.