2023-01-0037 Published 11 Apr 2023

A First Look at Android Automotive Privacy

Mert D. Pese Clemson University

Citation: Pese, M.D., "A First Look at Android Automotive Privacy," SAE Technical Paper 2023-01-0037, 2023, doi:10.4271/2023-01-0037.

Received: 22 Nov 2022 Revised: 13 Jan 2023 Accepted: 27 Jan 2023

Abstract

Android Automotive OS (AAOS) has been gaining popularity in recent years, with several OEMs across the world already deploying it or planning to in the near future. Besides the benefit of a well-known, customizable and secure operating system for OEMs, AAOS allows third-party app developers to offer their apps on vehicles of several manufacturers at the same time. Currently, there are 55 apps for AAOS that can be categorized as media, navigation or point-of-interest apps. Specifically the latter two categories allow the third-parties to collect certain sensor data directly from the vehicle. Furthermore, the latest version of AAOS also allows the OEM to configure and collect In-Vehicle Infotainment (IVI) and vehicle data (called OEM telemetry).

However, increasing connectivity and integration with the in-vehicle network comes at the expense of user privacy. Previous works have shown that vehicular sensor data often contains personally identifiable information (PII). New privacy regulations around the world mandate that the collection and processing of this data has to be clearly communicated with the user of the vehicle who reserves the right to approve or deny. In this paper, the existing AAOS apps are manually analyzed for the user data they collect and share. Of particular interest is the consistency of the declared app permissions with developers' privacy policies since discrepancies can suggest compliance issues. Our study results show that over 78% of analyzed apps do not mention all dangerous permissions in their privacy policies.

Introduction

Since the launch of Android Automotive OS (AAOS) in 2017, several automotive OEMs have identified the value of having a clean, established and developer-friendly in-vehicle infotainment (IVI) operating system. AAOS is an automotive-specific build of the mobile operating system Android and shares the vast majority of its codebase. Compared to Android Auto or Apple CarPlay which are running on the phone and merely mirror certain apps to the IVI screen, AAOS is running natively inside cars and can interact with the in-vehicle network (IVN), such as the CAN bus [5]. As a result, AAOS allows OEM and third-party apps to collect data from the IVN, opening new opportunities for third-party app developers, as well as data monetization possibilities. Currently, 13 vehicle models are already running or are planned to roll out AAOS on their IVIs [4]. Existing vehicle models comprise the Polestar 2 and Volvo XC40 from Geely Group, as well as several models from General Motors and Renault-Nissan-Mitsubishi. Other OEMs who have pledged to switch to AAOS include Ford, BMW, Stellantis and Honda in 2023. According to S&P Global's Feature Technology Benchmarking [4], the market share of AAOS among IVI operating systems is expected to grow from currently 1% to 18% by 2027 which will come at the expense of its competitors BlackBerry QNX [7] and Automotive Grade Linux [8].

AAOS is offered and maintained by Google and can come with Google apps and services, such as Google Maps, Assistant and the Play Store. All Google-branded apps are part of Google Automotive Services (GAS) which the majority of OEMs have opted to include in their AAOS production builds. An advantage for OEMs to license the GAS suite is access to the Google Play Store which allows third-party developers to distribute their apps to numerous vehicle models. With the fragmented landscape of legacy IVI operating systems, developers had to design their apps separately for each OS, reducing their visibility and facing increased development costs. However, since AAOS is an open-source operating system, OEMs can choose to provide it to their customers without purchasing a GAS license from Google as well. This route has been taken by Lucid Motors, Stellantis and BMW so far [4]. These OEMs can provide their own customized app environment without relying on apps such as Google Maps, offering a more unique brand experience. Another factor for ditching GAS could be to avoid sharing customer telemetry data with Google who could monetize it as part of their advertisement programs.

The collection of driver data will be enabled through AAOS. Three major stakeholders are Google through GAS, the OEM through their own services and apps bundled in the production builds, as well as third-party apps provided through the Google Play Store. There are 55 third-party apps that are available for AAOS as of November 2022, with 37 listed for all AAOS builds [3]. The other 18 apps can be found in the Play Stores of the Polestar 2 and Volvo XC40. Previous work has shown that automotive data is very rich and can be used for several applications ranging from EV maps to usage-based insurance (UBI), but raises serious privacy concerns [9]. Surveyed privacy attacks range from driver fingerprinting [10] and location inference attacks [11, 12] to driving-behavior analysis [13]. Increasing privacy regulation around the world forces OEMs to take customer privacy more seriously to avoid hefty fines. As an example, WhatsApp was fined €225 million in 2021 for its lack of transparency of user data handling [17]. The European Union (EU) has established a privacy standard called General Data Protection Regulation (GDPR) in May 2018 [14]. Although GDPR is only binding for EU residents and entities, OEMs are global companies selling cars worldwide. Hence, GDPR adherence is of great importance to North American OEMs. Even in the US, there are state-specific privacy laws, such as the California Consumer Privacy Act (CCPA) [15] and the more stringent 2023 update, the California Privacy Rights Act (CPRA) [16]. Both privacy legislations mandate a transparent and purposeful collection of user data. Since its inception, Android provides a permission model with predefined permissions [1]. Each installed application will request needed permissions. Before Android 6.0, these permissions were asked and granted during installation time. Newer Android versions require runtime permissions [18] for a specific set of sensitive Android permissions, with further iterations introduced in Android 10. In 2013, the Google Play Store started requiring app publishers to provide a link of their apps' privacy policies as part of their app approval process. Google requires certain sensitive permissions (dubbed *dangerous* permissions) such as location, microphone, etc. to be listed, together with why this data is collected. However, recent research has shown that Google only checks if a URL to a privacy policy has been included, but not its content [20]. Aforementioned study also shows that only 31% of third-party apps disclose all dangerous permissions in their privacy policies. Identifying inconsistencies between privacy policies and Android permissions can help fixing compliance issues and possible litigation.

In this paper, we analyzed 14 out of 55 third-party apps available on AAOS that are requesting car-related permissions (named *car apps* going forward). The vast majority of apps are media apps to stream online music. The study analyzes a total of 11 dangerous permission groups. Since there are only two automotive-specific dangerous permissions in AAOS, the analysis will also include other car-related permissions. In our study, we found that over 78% of analyzed apps do not mention all dangerous permissions in their privacy policies. We also discovered that 36% of apps circumvent the permission model by requesting signature permissions which are technically not given to third-party apps. Only 36% of car apps mention GDPR or CCPA in their privacy policies. All in all, we found that car apps in AAOS do not disclose permissions in their privacy policies very clearly and some of the apps can be seen as overprivileged. This can be explained mainly due to the novelty of car-specific permissions and the lack of understanding by developers.

Background

AAOS System Design

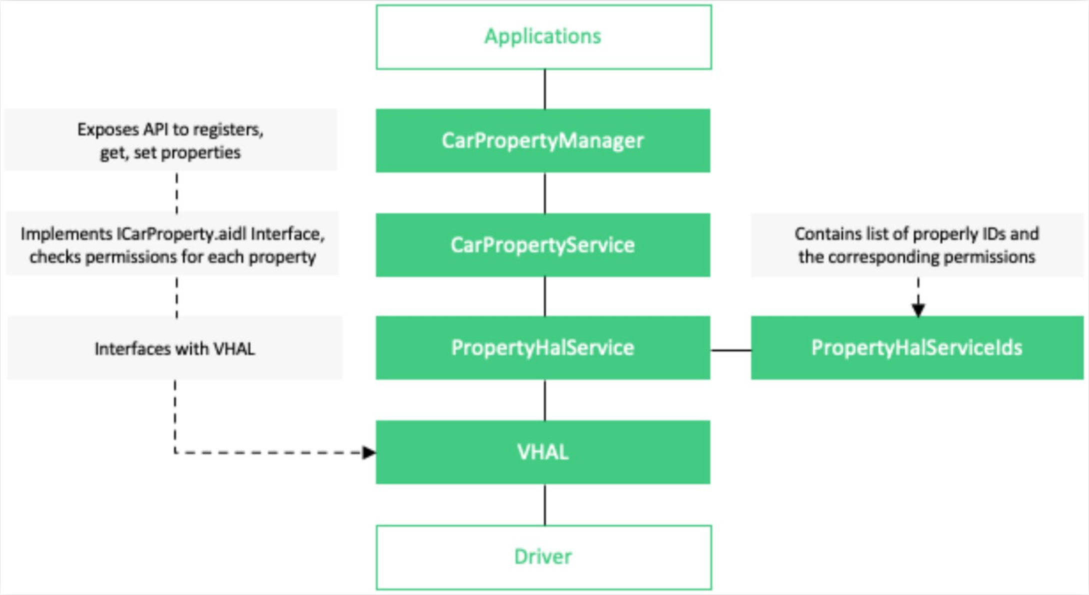
As mentioned in the introduction, AAOS introduces certain new modules to the regular Android system architecture to be able to interact with the vehicle. Since AAOS runs on the IVI ECU, it will have a direct connection to the in-vehicle network, such as the CAN bus. This is required for AAOS to be able to read and write data to it.

Figure 1 depicts the system architecture of AAOS. On the top, there are Android applications or services (called APKs from now on) which can have four origins:

- **AOSP**: These are APKs baked into the AAOS build by default since they are an essential part of the Android Open Source Project (AOSP). Most AOSP APKs provide basic services that are dependencies of other APKs (e.g., *com.android.carrierconfig*). Certain APKs can also be shared across different builds, independent of OEM customization (e.g., *com.android.car.systemupdater).*
- **Google**: These are APKs included by the OEM through Google Automotive Services (GAS). Examples are Google Maps (*com.google.android.apps.maps)* or Google Mobile Services (*com.google.android.gms*) to run Play Services.
- **OEM**: These are APKs provided by the car manufacturer (OEM) and are only part of the production build of their vehicles. Examples on the Polestar 2 are Audio Settings (*com.polestar.audiosettings*) or custom versions of generic AAOS third-party apps (e.g., com.polestar.abrp.production.android). The former are pre-installed whereas the latter can be downloaded from the Google Play Store.
- **Third-Party**: These are APKs that can be found in the Google Play Store (e.g., *net.vonforst.evmap*). These apps are usually shared across different production builds (and thus OEMs). There are 37 third-party apps that are listed generically for AAOS builds [3], although inspection of the Play Stores of production vehicles showed that additional third-party apps can be included. Google provides app developers resources on how to design and publish AAOS-specific apps [22] since they have to follow certain design guidelines to reduce distracted driving.

An exhaustive list of 55 AAOS APKs is provided in Table 5 (in Appendix). AOSP, Google and OEM apps are denoted as system apps in the following. All APKs interact with a CarManager instance which exposes the Application Programming Interface (API). There are multiple manager instances, e.g., a *CarHvacManager* that the OEM-provided HVAC APK can use. However, most APKs including

FIGURE 1 AAOS System Architecture (from [21])


Applications
CarPropertyManager
Exposes API to registers, get, set properties
CarPropertyService
Implements ICarProperty.aidl Interface, checks permissions for each property
Contains list of properly IDs and the corresponding permissions
PropertyHalService
Interfaces with VHAL
PropertyHalServiceIds
VHAL
Driver

third-party ones talk to the *CarPropertyManager* to get and set vehicle properties. The latter are defined in the Vehicle Hardware Abstraction Layer (VHAL) and abstract vehicle data from the IVN to APKs. Examples are powertrain-related data (e.g., speed, RPM, etc.), body-related data (e.g., windows, seats) or HVAC controls [6]. When an APK wants to read a vehicle property through the *CarPropertyManager*, the VHAL which interfaces the CAN driver for instance, will translate the CAN signal related to that vehicle property to an absolute value and pass it onto the *PropertyHalService*. The latter sits in between the VHAL and *CarPropertyManager* and is responsible for enforcing security. Vehicle properties are defined with read and write permissions that are required to get or set them, respectively [35]. For instance, the property *WINDOW_LOCK* requires the *CONTROL_CAR_WINDOWS* permission to be set. The service layer will restrict setting properties to system apps only to avoid arbitrary CAN injection attacks which can culminate in vehicle misbehavior. Furthermore, it is responsible for checking app-specific permissions which are explained next.

AAOS Permission Model

Android introduces a permission system with pre-defined permissions [1]. Every APK can request permissions and also define new permissions. For instance, Google Mobile Services (GMS), the parent of GAS, defines *com.google.android.gms.auth.permission.FACE_UNLOCK* which is not a standard AOSP permission. The device user has to grant APKs their requested permissions if they want to use them. Android permissions are divided into four protection levels [23]:

- **Normal:** Normal permissions (also known as install-time permissions) result in minimal risk to the user's privacy. If an app declares in its manifest that it needs a normal permission, the system automatically grants the app that permission at installation time without any explicit confirmation. Users cannot revoke these permissions.
- **Dangerous:** Dangerous permissions (also known as runtime permissions) are defined if the user's private information has to be accessed. If an app declares that it needs a dangerous permission, the user has to explicitly grant the permission to the app at installation time and/or its first launch. The app might not work properly if these permissions are not granted, e.g., a navigation app will not be able to locate the user.
- **Signature:** The system grants these app permissions at installation time, but only when the app is signed by the same certificate as the app that defines the permission. In the automotive domain, only OEM-native apps can use signature permissions.
- **signature|privileged:** These permissions are granted to either cryptographically signed or preinstalled apps. An OEM can assign permissions using this protection level to any third-party apps that it signs itself. These apps do not have to be preinstalled on the production build. For instance, Polestar provides the EasyPark APK with package name *com.polestar.easypark.production.android* that can theoretically request signature permissions. Volvo has the same APK in its Play Store with the package name *com.volvocars.easypark.production.android*. If the latter requested signature permissions, it would not be able to run on the Polestar, assuming that the Polestar and Volvo use different platform keys for signing.

All vehicle-specific permissions are defined in *android.car.permission* [2]. As of November 2022, 111 permissions are defined in AAOS. A selection of them is summarized in Table 1. This table shows all seven normal permissions, as well as the only two dangerous permissions that AAOS supports

TABLE 1 Selection of permissions defined in AAOS (android.car.permission) [2]

Permission Name	Protection Level	Description
READ_CAR_DISPLAY_UNITS	Normal	Allows an application to read the display units for distance, fuel, tire pressure, EV battery and fuel consumption.
CONTROL_CAR_DISPLAY_UNITS	Normal	Allows an application to control the display units for distance, fuel, tire pressure, EV battery and fuel consumption.
CAR_ENERGY_PORTS	Normal	Allows an application to read the vehicle fuel and charge port status.
CAR_INFO	Normal	Allows an application to read the vehicle car basic information. For example, it allows an application to read the vehicle Make, Model, Model Year, fuel capacity, fuel type, EV battery capacity, EV connection type, fuel door location and driver seat location.
CAR_EXTERIOR_ENVIRONMENT	Normal	Allows an application to read the vehicle exterior environment information. For example, it allows an application to read the vehicle exterior temperature and night mode status.
CAR_POWERTRAIN	Normal	Allows an application to read the vehicle powertrain information. For example, it allows an application to read the vehicle current gear, ignition state or parking brake status.
READ_CAR_POWER_POLICY	Normal	Allows an application to get the current power policy or to be notified of power policy change.
CAR_SPEED	Dangerous	Allows an application to read the vehicle speed.
CAR_ENERGY	Dangerous	Allows an application to read the vehicle energy information.
CAR_IDENTIFICATION	signature|privileged	Allows an application to read the VIN information.
CAR_MILEAGE	signature|privileged	Allows an application to read the vehicle mileage information.
CAR_ENGINE_DETAILED	signature|privileged	Allows an application to read the vehicle engine information. For example, it allows an application to read the engine oil level, oil temperature, coolant temperature and RPM.
CAR_VENDOR_EXTENSION	signature|privileged	Allows an application to access the vehicle vendor channel to exchange vendor-specific information.
READ_CAR_INTERIOR_LIGHTS	signature|privileged	Allows an application to read the vehicle interior lights state.
CAR_NAVIGATION_MANAGER	signature|privileged	Allows an application to access {@link android.car.navigation.CarNavigationStatusManager} to report navigation data. This information may be displayed by the vehicle in the instrument cluster, head-up display or other locations.

today. There are 102 signature|privileged permissions and six of them which are related to the findings of our privacy analysis in this paper are listed, together with a brief description of each permission. Third-party apps will either use normal or dangerous permissions, with the exception of the OEM signing the app as explained above. Signature permissions are normally limited to system apps, i.e., a regular app cannot access HVAC settings or control body functions such as the seats or windows. Currently, most permissions are signature or privileged. The only dangerous permissions at this time that require explicit user consent are speed and some more information about the vehicle's energy state. Nevertheless, several powertrain-related information, such as gear position or engine speed (RPM) are available to anyone without explicit permission.

Privacy Regulation

As mentioned in Sec. 1, there are several new privacy regulations that have been passed in recent years. The General Data Protection Regulation (GDPR) is the most comprehensive of them and will affect all global carmakers conducting business in the European Union. GDPR distinguishes between data subjects, data controllers and data processors. GDPR ensures adequate protection of the privacy rights of data subjects, i.e., drivers in our context. Data controllers dictate how and why data is going to be used by the organization and thus have the most responsibility when it comes to protecting the privacy and rights of the data subject. Data processors process any data on behalf of the data controller. Since OEMs control the data shared with third-party app providers, they fall under the category of data controllers and are subject to increased compliance obligations. These are summarized as seven core principles in the following [24]:

1. **Lawfulness, Fairness and Transparency**: Relates to the legality of data collection and transparency of users' collected data.
2. **Purpose Limitation**: Use collected data only for the specific purposes for which it was collected.
3. **Data Minimization**: Only request data that is required for a purpose.
4. **Accuracy**: Relates to upkeeping the accuracy and completeness of such data and what a consumer's rights are for correcting inaccuracies.
5. **Storage Limitation**: Constrain the amount of time that personal data can be stored for.

6. **Integrity and Confidentiality**: Relates to security of data transmission and storage, e.g., by encrypting and pseudonymizing data.
7. **Accountability**: Have appropriate measures and records in place to take responsibility for what you do with personal data and how you comply with the other principles.

The Android framework consisting of permission model and mandatory privacy policies is available to address GDPR principles (1), (3), (4), (6) and (7). Although the privacy policies of an APK can include provisions on how personal data will be used and how long it will be stored on the third-party backend, AAOS has no real control over these points. Although some third-party apps include information about purpose and storage limitations, Google does not officially require them in an app's privacy policy [25]. The only categories required are if ads and authentication are used, information about the target audience and content, requested dangerous permissions, as well as content ratings.

Besides GDPR, the California Consumer Privacy Act (CCPA) is the first large privacy law enacted in the US, although it applies only to residents of California. The most important difference from GDPR is prior consent versus opting out [26]. GDPR requires users to give clear and affirmative consent prior to having data collected and processed. CCPA requires businesses to make it possible for consumers to opt out of having data disclosed or sold to third-parties. Among others, the definition of "businesses" was quite vague in the original definition of CCPA. To overcome these ambiguities, CCPA was amended to form the California Privacy Rights Act (CPRA) [27].

Experimental Design

Obtaining the APKs

The most straightforward way to obtain a large number of APKs is to develop a scraper to search online on APK mirror websites [29] and download them in an automated fashion such as previous work has suggested [20]. APKs are officially only found on the Google Play Store and can be installed by the user onto their device. After downloading and installing an APK through the Play Store, the APKs are usually stored in the /data/app/ directory of the Android file system. Contributors to APK mirror websites can extract these APKs from the file system by using the built-in file manager or APK extractor tools [30].

The Google Play Store website for AAOS lists 37 apps [3]. However, when we searched these APKS on the most popular APK mirror websites, we found out that none of these apps were available. The most likely explanation is that nobody made the effort to extract these apps from their IVIs yet, mostly because of low market share, as well as harder access to the device compared to a mobile phone. As a result, we had to perform the steps of installing the APK from the Play Store onto an AAOS device and extracting the APK ourselves. Since finding one of the few AAOS-powered vehicles [4] is difficult, we decided to use available AAOS emulators, specifically the Polestar 2 [31] and Volvo VX40 Recharge [32] that are publicly available online. The OEMs have released these emulator images for third-party app developers to test their apps on an AAOS production build. Although it is possible to build an AAOS emulator image from the Android Open-Source Project (AOSP), these development builds lack Google Automotive Services (GAS) and thus access to the Play Store. In both production builds, the Play Store was pre-installed and we could log in with a Google account and install all available third-party apps. During our analysis, we found out that Polestar 2 contains an additional 16 apps (and Volvo XC40 an additional two apps on top of it) compared to the official Play Store listing [3], yielding a total of 55 APKs. Next, we used an Android developer tool, namely the Android Debug Bridge (ADB), to interact with the file system of the running emulator. We first located the path of all installed packages (*adb shell pm list packages -f*) and then downloaded them to our local file system (*adb pull*). Note that no root access is required to perform these steps.

Manifest Analysis

As described before, the objective of this paper is to analyze if the privacy policies of AAOS third-party APKs are consistent with their requested permissions. The latter are declared in the Android Manifest, an XML file that is part of the APK, besides the program code, resources, assets and certificates. APKs can be regarded as an archive that has to be unzipped first. Reverse-engineering tools such as apktool [28] can decode APKs to their nearly original form, effectively yielding the manifest file. Permissions are relatively fine-grained and there are 31 dangerous permissions in Android [1]. It can be hard to match each fine-grained permission to the natural language text in a privacy policy. As a result, these 31 permissions are logically grouped into 11 permission groups in accordance with previous work [20]. Table 2 depicts the grouping. Note that there are 29 distinct dangerous permissions in Android that are not car-specific. AAOS apps also request non-car-specific permissions, e.g., location, that is used in several navigation apps. The permissions for location are shared with non-automotive Android builds as well.

After extracting the permissions from the Android manifests, we first selected all dangerous permissions and mapped them to permission groups according to Table 2. The left hand side of Figure 2 shows that among 55 analyzed AAOS APKs, the top three dangerous permission groups were *PERSISTENTID* (94.5%), *LOCATION* (43.6%) and *STORAGE* (34.5%). *CAR_MONITORING* which only includes the permission *CAR_ENERGY* (since *CAR_SPEED* is mapped to *LOCATION*) comes at number five with only 14.5%. Unsurprisingly, *SMS*, *PHONE_CALL*, *CALENDAR* and *CAMERA* are the least accessed permission groups given that AAOS is running on an IVI ECU without camera, calendar or telephony capabilities. To support this, we investigated the two production builds that we analyzed (Polestar 2 and Volvo XC40), and there were no dialer, camera or calendar apps installed (although AAOS contains a hardware abstraction layer for the exterior view system [33], such as back-up camera,

TABLE 2 List of Android dangerous permissions in 11 permission groups [1]

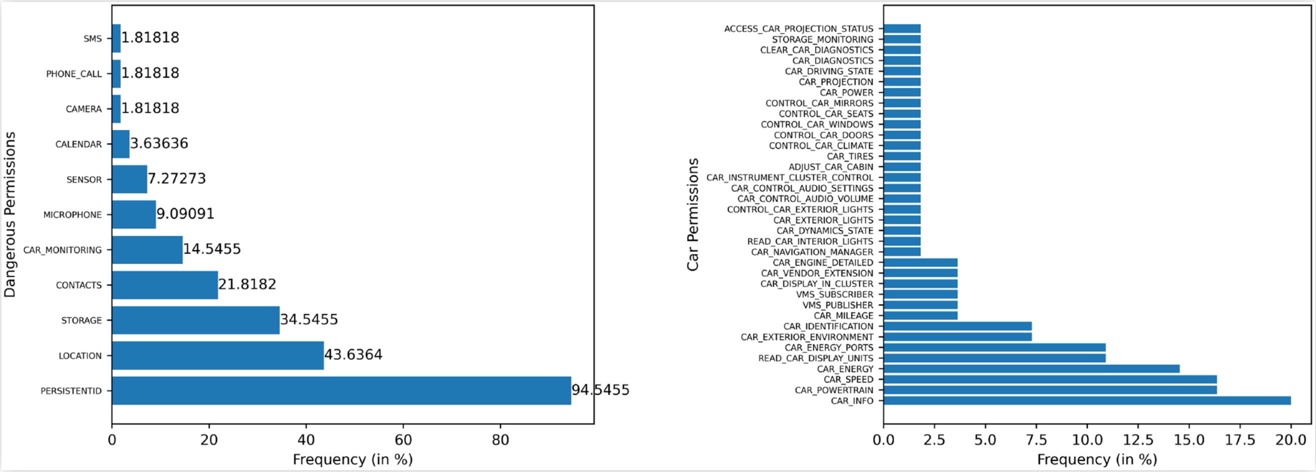
Dangerous Permissions	Permission Group
READ_CALENDAR	CALENDAR
WRITE_CALENDAR	
CAR_ENERGY	CAR_MONITORING
CAMERA	CAMERA
READ_CONTACTS	CONTACTS
WRITE_CONTACTS	
GET_ACCOUNTS	
ACCESS_FINE_LOCATION	LOCATION
ACCESS_COARSE_LOCATION	
ACCESS_MEDIA_LOCATION	
ACCESS_BACKGROUND_LOCATION	
CAR_SPEED	
RECORD_AUDIO	MICROPHONE
READ_PHONE_STATE	PERSISTENTID
ACCESS_NETWORK_STATE	
READ_PHONE_NUMBERS	PHONE_CALL
CALL_PHONE	
ANSWER_PHONE_CALLS	
ADD_VOICEMAIL	
USE_SIP	
READ_CALL_LOG	
WRITE_CALL_LOG	
PROCESS_OUTGOING_CALLS	
ACTIVITY_RECOGNITION	SENSOR
BODY_SENSORS	
SEND_SMS	SMS
RECEIVE_SMS	
RECEIVE_WAP_PUSH	
RECEIVE_MMS	
READ_EXTERNAL_STORAGE	STORAGE
WRITE_EXTERNAL_STORAGE	

that third-party apps are not supposed to connect to). We traced back the *CAMERA* permission to A Better Route Planner (*com.polestar.abrp.production.android*) which already seems overprivileged. The same applies to the *CALENDAR* permission which are both requested by *com.polestar.abrp.production.android* and *nl.flitsmeister*. We also found out that the *SMS* and *PHONE_CALL* permissions are requested by the Google Assistant for AAOS (*com.google.android.carassistant*) which looked legitimate at first sight. On the right hand side of Figure 2, we listed the relative frequency of all car-specific fine-grained permissions (denoted with prefix *android.car.permission* instead of *android.permission*). 1 in 5 APKs requested basic information about the vehicle (*CAR_INFO*), with 1 in 6 APKs using the dangerous *CAR_SPEED* permission. The low percentage of apps requesting car-specific permissions can be explained by the majority of media apps among the 55 AAOS APKs. As Table 5 (in Appendix) shows, only 10 apps are categorized as Maps & Navigation and *actually* collect data from the vehicle. Media apps (grouped as Music & Audio, Entertainment, News & Magazines, Books & References) are mostly only using the non-sensitive Internet permission and are not interesting for further analysis. Including the aforementioned 10 Maps & Navigation apps, we were interested in taking a closer look at a total of 14 APKs as described next.

Privacy Policy Analysis

For the 14 APKs of interest, our objective was to extract information about sensitive data collection from the privacy policy URLs provided by the app developers in the Google Play Store. Recall that only dangerous permissions are required to be included in the natural language policy text. Due to the low number of APKs (and thus privacy policies), the author decided to go through the URLs manually and extract permission groups. Note that due to the subjectivity of the manual analysis, there might be bias and/or human error. To minimize these, the author invited a second human subject who is familiar with AAOS to repeat the process. This way,

FIGURE 2 Left: Distribution of dangerous permissions in 55 AAOS third-party APKs, Right: Distribution of car-related permissions in 55 AAOS third-party APKs



discrepancies between the two human interpretations could be identified and eliminated to improve the quality of the manual privacy policy analysis. In accordance with previous work [20], the human subjects agreed on a set of rules to follow while extracting permission groups:

- Human subjects mark direct references to the 11 permission groups from Table 2. Note that we use the more coarse-grained permission groups instead of the fine-grained permissions.
- No human subject was allowed to look at the Android Manifests of the APKs beforehand to avoid bias.
- We focused on dangerous permissions from the aforementioned 11 permission groups, but also wanted to identify *any* car-related permission. For this purpose, human subjects made themselves familiar with normal, dangerous and signature permissions from the *android.car.permission* package (see Table 1).
- Human subjects were focusing on the data collection from the device (i.e., IVI/car) and not user registration process which was explained in numerous privacy policies as well.
- Human subjects analyze indirect references to the 11 permission groups by replicating app features. For instance, if an APK mentions creating a data log with collected data, it is likely that the log is going to be stored on the device. As a result, the APK will request the *WRITE_EXTERNAL_STORAGE* permission and the human subjects will mark the permission group *STORAGE*.

Both human subjects had an overlap of more than 95% in their respective analyses. The remaining discrepancies were discussed to derive the final experimental evaluation which is presented in the next section.

Experimental Evaluation

The extracted car-specific permissions from Android Manifests, as well as privacy policies are displayed in Table 3 (normal and dangerous protection level) and Table 4 (signature protection level). The marker ‘X’ in a cell indicates that the respective permission is present in the manifest or the privacy policy. All 14 APKs were chosen out of 55 available AAOS apps because they declared at least one car-specific permission. Two exceptions to this rule were the Google Assistant for AAOS (*com.google.android.carassistant*) and Google Play Services (*com.google.android.gms*) since they requested nearly every car-specific permission and are technically system apps. A red marker ‘X’ indicates that a dangerous or signature permission is present in the manifest, but not in the privacy policy. The last columns of Tables 3 and 4 indicate the total number of permission discrepancies for each respective app. For completeness, Table 6 (in Appendix) lists the other dangerous permissions and indicates if the APK mentions GDPR or CCPA compliance in their respective privacy policy. In the following, we are summarizing the findings from our study.

Findings

- **Dangerous permissions are usually not explained in privacy policies**: Unfortunately, only 3 of the 14 analyzed APKs (21%) have a complete description of all dangerous permissions that they have declared in their respective Android Manifests. This compares to 31% for smartphone Android apps as shown in prior work [20]. As a result, privacy policies of AAOS apps are even more inconsistent than their smartphone counterparts. However, out of 12 apps that request *LOCATION*, 92% mention it in their privacy policies. This number stands at 86% for *PERSISTENTID*, 50% for *SENSOR*, 43% for *CAR_ENERGY*, 40% for *STORAGE* and 25% each for *CAR_SPEED* and *CONTACTS*, respectively. Not a single APK that requests *CAMERA*, *CALENDAR* or *MICROPHONE* mention these permissions in their privacy policies. Given the lack of camera or calendar in IVIs, there is absolutely no reason why these permissions are requested in the first place by certain APKs. A lower ratio for car-specific dangerous permissions can be acknowledged for now due to the novelty of AAOS and possible lack of understanding by developers. However, speed is a very sensitive parameter that can be used to infer the driver’s taken trips [11, 12] and needs to be highlighted more in privacy policies.
- **Normal car-specific permissions are sometimes mentioned in privacy policies**: Although normal permissions are not required to be disclosed in privacy policies, Table 3 shows that some permissions are being discussed by developers. The median of 37.5% among the five car-specific normal permissions is low, but comparable to the median of car-specific dangerous permissions.
- **Apps declare signature permissions**: Table 4 shows that 5 out of 14 analyzed APKs (36%) declare signature permissions in their Android Manifest. As explained in the Background section, third-party APKs are only allowed to request normal or dangerous permissions. However, if an APK is cryptographically signed with the OEM (or Google) key, it can request signature permissions. As can be seen from Table 4, three APKs are signed by Polestar (i.e., the OEM) and one APK by Google. However, *com.sygic.aura* requests *CAR_MILEAGE* which is a signature permission and the APK is not signed by neither the OEM nor Google. Furthermore, the APK signature suggests that the app has been signed by the app developer Sygic. It is unclear how this APK made its way to the Google Play Store and what the app behavior will look like (since we did not conduct a dynamic analysis).
- **Average number of discrepancies is high**: Tables 3, 4 and 6 show the total number of permission discrepancies between the manifest and privacy policy. For car-specific dangerous permissions (see Table 3), the average number of discrepancies stands at 0.71 (out of 2 dangerous permissions). This translates to nearly 36% of car-specific dangerous permissions to be missing in privacy policies. After adding non-car-specific dangerous permissions (see Table 6), the average number increases to 1.78 (out of

TABLE 3 Permission analysis for car-specific normal and dangerous protection level

Package Name	Permission Declared	READ_CAR_DISPLAY_UNITS	CAR_ENERGY_PORTS	CAR_INFO	CAR_EXTERIOR_ENVIRONMENT	CAR_POWERTRAIN	CAR_ENERGY	CAR_SPEED	# Discrepancies
com.polestar.abrp.production.android	Manifest		X	X	X	X	X	X	0
	Privacy Policy		X	X	X		X	X	
com.polestar.easypark.production.android	Manifest					X	X		1
	Privacy Policy								
com.sygic.aura	Manifest	X				X	X		0
	Privacy Policy						X		
com.xatori.Plugshare	Manifest	X		X				X	1
	Privacy Policy								
com.parkwhiz.driverApp	Manifest								0
	Privacy Policy								
com.coulombtech	Manifest		X	X		X	X	X	1
	Privacy Policy							X	
nl.flitsmeister	Manifest								0
	Privacy Policy								
com.spothero.spothero	Manifest								0
	Privacy Policy			X					
com.google.android.apps.maps	Manifest	X		X			X	X	2
	Privacy Policy								
com.polestar.driver.journey.log.production.android.apk	Manifest	X	X	X	X	X	X	X	1
	Privacy Policy		X			X		X	
com.polestar.spacewarp.production.android	Manifest					X			0
	Privacy Policy			X	X	X	X	X	
com.polestar.p2performancepack.production.android	Manifest			X	X	X	X	X	2
	Privacy Policy								
com.polestar.web.production.android	Manifest			X		X			0
	Privacy Policy			X		X			
net.vonforst.evmap	Manifest	X	X	X			X	X	2
	Privacy Policy			X					

TABLE 4 Permission analysis for car-specific signature protection level

Package Name	Permission Declared	CAR_ IDENTIFICATION	CAR_MILEAGE	CAR_ENGINE_ DETAILED	CAR_ VENDOR_ EXTENSION	CAR_ NAVIGATION_ MANAGER	READ_CAR_ INTERIOR_ LIGHTS	# Discrepancies
com.polestar.abrp. production.android	Manifest	X						1
	Privacy Policy							
com.polestar.easypark. production.android	Manifest							0
	Privacy Policy							
com.sygic.aura	Manifest		X					1
	Privacy Policy							
com.xatori.Plugshare	Manifest							0
	Privacy Policy							
com.parkwhiz.driverApp	Manifest							0
	Privacy Policy							
com.coulombtech	Manifest							0
	Privacy Policy							
nl.flitsmeister	Manifest							0
	Privacy Policy							
com.spothero.spothero	Manifest							0
	Privacy Policy							
com.google.android.apps. maps	Manifest					X		1
	Privacy Policy							
com.polestar.driver.journey. log.production.android.apk	Manifest	X					X	2
	Privacy Policy							
com.polestar.spacewarp. production.android	Manifest							0
	Privacy Policy	X						
com.polestar. p2performancepack. production.android	Manifest	X		X	X			3
	Privacy Policy							
com.polestar.web.production. android	Manifest							0
	Privacy Policy							
net.vonforst.evmap	Manifest							0
	Privacy Policy							

11 dangerous permissions). All in all, over 16% of dangerous permissions overall are never mentioned in privacy policies.

- **Duplicate permission definition**: In the analysis of the 55 AAOS APKs, we found that certain permissions are defined twice, e.g., *android.car.permission.CAR_SPEED* and *com.google.android.gms.permission.CAR_SPEED*. The latter is a re-declaration of the *CAR_SPEED* permission by Google Play Services (i.e., GAS) with signature protection level. Only two apps request the custom GAS permission, namely *net.vonforst.evmap* and *com.google.android.apps.maps*. Both apps also request the regular CAR_SPEED permission at the same time. It is not clear what the difference between these two permission definitions are, especially given because custom permissions lack any public documentation. Even if the duplicate permission declaration cannot be understood for Google Maps, the other third-party APK's behavior specifically raises questions and concerns.
- **Some apps mention permissions in privacy policy, but do not declare in manifest**: Contrary to the original purpose of this paper, certain privacy policies suggest the declaration of permissions that are not part of the Android Manifest. For instance, the privacy policy URL of *com.polestar.spacewarp.production.android* states that data related to "driving data (vehicle speed, brake and accelerator pedal use, steering wheel movement, etc.)" might be collected, although none of these car-specific permissions are requested in the manifest. These rarities are benign from a privacy perspective and can be explained by app developers often using cookie-cutter templates [20].
- **Indication of GDPR/CCPA compliance**: Finally, we searched privacy policies for presence of GDPR or CCPA keywords. 5 out of 14 analyzed APKs mention these regulations respectively. It is interesting that only one app (*com.xatori.Plugshare*) mentions both, whereas the others only mention one. This can be explained by the developers' home country, with US developers leaning towards talking about CCPA and Europeans towards GDPR.

Summary/Conclusions

In this paper, we surveyed the Android Automotive application landscape and conducted a first privacy analysis of 55 apps that exist up-to-date. The vast majority of apps consist of media apps that do not interact with the in-vehicle network. We analyzed the remaining 14 apps of interest to find that various data is collected from cars. App developers are not very consistent nor transparent in explaining sensitive permissions to users. In fact, our study showed that over 78% of analyzed apps do not mention all dangerous permissions in their privacy policies. Furthermore, at least two third-party apps were clearly overprivileged by requesting unnecessary permissions for their purposes, such as camera or calendar. As part of future work, we want to analyze potentially overprivileged apps in more detail by performing static and dynamic analyses of the APKs. This will allow us to see when and why declared permissions are used. With increasing collection and awareness of vehicular sensor data, e.g., through the newly introduced OEM telemetry feature in Android 13 [35], we expect that app developers will improve their privacy policies' compliance and completeness in the near future.

References

1. Android Developers, "Manifest.permission &nbsp;: &nbsp; Android Developers," accessed November 10, 2022, https://developer.android.com/reference/android/Manifest.permission
2. Google Git, "Service/Androidmanifest.xml - Platform/Packages/Services/Car - Git at Google," accessed November 10, 2022, https://android.googlesource.com/platform/packages/services/Car/+/master/service/AndroidManifest.xml
3. Google, "Android Apps on Google Play," accessed November 10, 2022, https://play.google.com/store/apps/collection/promotion_android_auto_embedded_exploreall?clp=CjIKMAoqcHJvbW90aW9uX2FuZHJvaWRfYXV0b19lbWJlZGRlZF9leHBsb3JlYWxsEEoYAw%3D%3D%3AS%3AANO1ljJ6-L0&amp;gsr=CjQKMgowCipwcm9tb3Rpb25fYW5kcm9pZF9hdXRvX2VtYmVkZGVkX2V4cGxvcmVhbGwQShgD%3AS%3AANO1ljKPhR8
4. S&P Global, "Sharing Insights Elevates Their Impact." November 11, 2022, https://www.spglobal.com/mobility/en/research-analysis/android-automotive-is-taking-over-but-what-about-google.html
5. Ron Amadeo - May 10, 2021 11:15 am UTC, "Android Automotive OS Review: Under the Hood with Google's Car Os," Ars Technica, May 10, 2021, https://arstechnica.com/cars/2021/05/android-automotive-os-review-under-the-hood-with-googles-car-os/4/
6. Pese, M., Shin, K., Bruner, J., and Chu, A., "Security Analysis of Android Automotive," *SAE Int. J. Adv. & Curr. Prac. in Mobility* 2, no. 4 (2020): 2337-2346.
7. BlackBerry QNX, "Embedded OS, Support and Services: RTOS, Hypervisor," accessed November 10, 2022, https://blackberry.qnx.com/en
8. Automotive Grade Linux, "Home," November 16, 2022, https://www.automotivelinux.org/
9. Pesé, M.D. and Shin, K.G., "Survey of Automotive Privacy Regulations and Privacy-Related Attacks," SAE Technical Paper 2019-01-0479 (2019, 2019), https://doi.org/10.4271/2019-01-0479.
10. Enev, M. et al., "Automobile Driver Fingerprinting," *Proceedings on Privacy Enhancing Technologies* 1 (2016): 34-50.
11. Dewri, R., Annadata, P., Eltarjaman, W., and Thurimella, R., "Inferring Trip Destinations from Driving Habits Data," in *Proceedings of the 12th ACM Workshop on Privacy in the Electronic Society*, 267-272, November 2013. ACM.

12. Pesé, M.D., Pu, X., and Shin, K.G., "SPy: Car Steering Reveals Your Trip Route!" *Proc. Priv. Enhancing Technol.* 2020, no. 2 (2020): 155-174.

13. Kaplan, S., Guvensan, M.A., Yavuz, A.G., and Karalurt, Y., "Driver Behavior Analysis for Safe Driving: A Survey," *IEEE Transactions on Intelligent Transportation Systems* 16, no. 6 (2015): 3017-3032.

14. "The EU General Data Protection Regulation (GDPR) is the Most Important Change in Data Privacy Regulation in 20 Years," https://eugdpr.org/

15. "Basics of the California Consumer Privacy Act of 2018," https://www.privacypolicies.com/blog/california-consumer-privacy-act/

16. California Consumer Privacy Act (CCPA), https://www.cookiebot.com/en/ccpa-compliance/

17. BBC, "WhatsApp Issued Second-Largest GDPR Fine of 225m—BBC News," accessed November 11, 2022, September 2021, https://www.bbc.com/news/technology-58422465

18. Android Open Source Project, "Runtime Permissions &nbsp;: &nbsp; Android Open Source Project," accessed November 10, 2022, https://source.android.com/docs/core/permissions/runtime_perms

19. Harris, K., "Privacy on the Go—Recommendations for the Mobile Ecosystem," accessed: November 18, 2022, January 2013, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf

20. Rahman, M.S., Naghavi, P., Kojusner, B., Afroz, S. et al., "PermPress: Machine Learning-Based Pipeline to Evaluate Permissions in App Privacy Policies," *IEEE Access* 10 (2022): 89248-89269.

21. "Android Automotive and Physical Car Interaction: Android Automotive OS Book," Android Automotive OS Book | Build Your Infotainment System Based on Android Automotive OS, September 3, 2020, https://www.androidautomotivebook.com/android-automotive-and-physical-car-interaction/

22. Android Developers, "Distribute Android Apps for Cars &nbsp;: &nbsp; Android Developers," accessed November 10, 2022, https://developer.android.com/training/cars/distribute

23. Android Developers, "Permissions on Android &nbsp;: &nbsp; Android Developers," accessed November 10, 2022, https://developer.android.com/guide/topics/permissions/overview

24. Özkan, I., "Data Protection Principles: The 7 Principles of GDPR Explained," CyberPilot, November 14, 2022, https://www.cyberpilot.io/cyberpilot-blog/data-protection-principles-the-7-principles-of-gdpr-explained/

25. Google, "Prepare Your App for Review - Play Console Help," accessed November 11, 2022, https://support.google.com/googleplay/android-developer/answer/9859455?hl=en

26. "CCPA VS GDPR: Compliance with Cookiebot CMP," accessed November 10, 2022, https://www.cookiebot.com/en/ccpa-vs-gdpr-compliance-with-cookiebot-cmp/

27. "California Privacy Rights Act (CPRA): CCPA VS CPRA," accessed November 10, 2022, https://www.cookiebot.com/en/cpra/

28. "Apktool," Apktool - A Tool for Reverse Engineering 3rd Party, Closed, Binary Android Apps, accessed November 11, 2022, https://ibotpeaches.github.io/Apktool/

29. APKMirror, "Free APK Downloads - Free and Safe Android APK Downloads," accessed November 11, 2022, https://www.apkmirror.com/

30. APKMirror, "ML Manager: APK Extractor Apks," accessed November 11, 2022, https://www.apkmirror.com/apk/javier-santos-v/ml-manager-apk-extractor/

31. "Developer Portal," accessed November 11, 2022, https://www.polestar.com/us/developer/get-started/

32. Volvo Cars Developer Portal, "Android Emulator – in-Car Apps," accessed November 11, 2022, https://developer.volvocars.com/in-car-apps/android-emulator-xc40/

33. Android Open Source Project, "Vehicle Camera Hal &nbsp;: &nbsp; Android Open Source Project," accessed November 11, 2022, https://source.android.com/docs/devices/automotive/camera-hal

34. Android Open Source Project, "Android Automotive 13 Release Details &nbsp;: &nbsp; Android Open Source Project," aAccessed November 12, 2022, https://source.android.com/docs/devices/automotive/start/t_release

35. Android Developers, "VehiclePropertyIds : Android Developers," accessed January 12, 2023, https://developer.android.com/reference/android/car/VehiclePropertyIds

Contact Information

Mert D. Pesé, Ph.D.
Clemson University
215 McAdams Hall, 821 McMillan Rd, Clemson, SC 29631
mpese@clemson.edu

Definitions/Abbreviations

AAOS - Android Automotive Operating System

AOSP - Android Open Source Project

ADB - Android Debug Bridge

APK - Android Package

OEM - Original Equipment Manufacturer

ECU - Electronic Control Unit

PII - Personally Identifiable Information

IVI - In-Vehicle Infotainment

IVN - In-Vehicle Network

CAN - Controller Area Network

GAS - Google Automotive Services

GMS - Google Mobile Services

EV - Electric Vehicle

UBI - Usage-Based Insurance

GDPR - General Data Protection Regulation

CCPA - California Consumer Privacy Act

API - Application Programming Interface

VHAL - Vehicle Hardware Abstraction Layer

HVAC - Heating, Ventilation and Air Conditioning

Appendix

TABLE 5 All 55 Android Automotive Apps with package names, link to their privacy policy URL and category on Google Play Store. 37 white-shaded apps are listed on Google Play Store website for all AAOS-enabled cars [3], 16 gray-shaded apps are available on Polestar 2 (all apps minus Polestar apps also available on Volvo XC40), 2 blue-shaded apps only available on Volvo XC40

App Name	Package Name	Privacy Policy URL	Category
A Better Routeplanner (ABRP)	com.polestar.abrp.production.android	https://www.iternio.com/integrity-policy https://forum.abetterrouteplanner.com/privacy/	Maps & Navigation
EasyPark - Keep Moving	com.polestar.easypark.production.android	https://legals.easyparksystem.net/SE/privacy/en/privacy_se_en.pdf	Maps & Navigation
Sygic GPS Navigation & Maps	com.sygic.aura	https://www.sygic.com/company/privacy-policy	Maps & Navigation
PlugShare - EV & Tesla Map	com.xatori.Plugshare	https://company.plugshare.com/privacy-and-terms-embed.html	Maps & Navigation
ParkWhiz -- Parking App	com.parkwhiz.driverApp	https://www.parkwhiz.com/support/terms/	Maps & Navigation
ChargePoint	com.coulombtech	https://na.chargepoint.com/privacy_policy	Maps & Navigation
Amazon Music	com.amazon.mp3.automotiveOS	https://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=468496&ref_=footer_privacy	Music & Audio
Flitsmeister	nl.flitsmeister	https://www.flitsmeisterapp.com/#/en/privacy https://4411.io/nl-nl/privacy-policy	Maps & Navigation
SpotHero - Find Parking	com.spothero.spothero	https://spothero.com/legal/privacy-policy	Maps & Navigation
LiveOne: Stream Music & Events	com.slacker.radio	https://www.liveone.com/privacy	Music & Audio
Spotify: Music and Podcasts	com.spotify.music	https://www.spotify.com/us/legal/privacy-policy/	N/A
Vivaldi	com.polestar.vivaldi.production.android	N/A (no data collected)	Tools
Tidal Music	com.aspiro.tidal	https://tidal.com/privacy	Music & Audio
NPR One	org.npr.one	https://www.npr.org/about-npr/179878450/privacy-policy	News & Magazines
YouTube Music	com.google.android.apps.youtube.music	https://policies.google.com/privacy	N/A
BBC Sounds: Radio & Podcasts	com.bbc.sounds	https://www.bbc.co.uk/usingthebbc/privacy	Music & Audio
Google Automotive Keyboard	com.google.android.apps.automotive.inputmethod	https://policies.google.com/privacy	Productivity
Pocket Casts - Podcast Player	au.com.shiftyjelly.pocketcasts	https://support.pocketcasts.com/article/privacy-policy/	News & Magazines
Google Maps	com.google.android.apps.maps	https://policies.google.com/privacy	Maps & Navigation
Audioburst - AAOS: Short, pers	com.audioburst.automotive	N/A (no information available)	Music & Audio
myCANAL, TV en live et replay	com.canal.android.canal	https://static.canalplus.com/legal/donnees-personnelles.html	Entertainment
iHeart: Music, Radio, Podcasts	com.clearchannel.iheartradio.controller	https://www.iheart.com/content/privacy-and-cookie-notice/	Music & Audio
Google Play Books & Audiobooks	com.google.android.apps.books	https://policies.google.com/privacy	N/A
Google Assistant - in the car	com.google.android.carassistant	https://policies.google.com/privacy	Tools
Google Play services	com.google.android.gms	https://policies.google.com/privacy	N/A
AudioCrate Remote	com.neleso.audiocrate	N/A (no information available)	Auto & Vehicles

(continued)

TABLE 5 (Continued) All 55 Android Automotive Apps with package names, link to their privacy policy URL and category on Google Play Store. 37 white-shaded apps are listed on Google Play Store website for all AAOS-enabled cars [3], 16 gray-shaded apps are available on Polestar 2 (all apps minus Polestar apps also available on Volvo XC40), 2 blue-shaded apps only available on Volvo XC40

App Name	Package Name	Privacy Policy URL	Category
Libby, by OverDrive	com.overdrive.mobile.android.automotive.libby	https://company.cdn.overdrive.com/policies/privacy-policy.htm	Books & Reference
Radio FM	com.radio.fmradio	https://appradiofm.com/privacy-policy	Music & Audio
Radio France : radios, podcast	com.radiofrance.radio.radiofrance.android	https://www.radiofrance.com/politique-d-utilisation-des-cookies-sur-les-sites-internet-du-groupe-radio-france	Music & Audio
Open Radio	com.yuriy.openradio	N/A (no data collected)	Music & Audio
ARD Audiothek	de.ard.audiothek	https://www.ardaudiothek.de/datenschutz/	Music & Audio
radio.net - radio and podcast	de.radio.android	https://www.radio.net/privacy_android_en_US	N/A
Trebble FM - Daily shortcasts	fm.trebble	https://www.trebble.fm/trebble-fm-inc-privacy-policy	News & Magazines
Brony Radio for Automotive	nl.frankkie.bronyradio.automotive	N/A (no information available)	Music & Audio
NRK Radio	no.nrk.mobil.radio	https://www.nrk.no/retningslinjer/ivaretakelse-av-personvern-i-nrks-plattformavhengige-apper-1.12823118	Music & Audio
Sveriges Radio Play	se.sr.android	https://sverigesradio.se/artikel/integritetspolicy-for-sveriges-radio-play	News & Magazines
TuneIn Radio: News, Music & FM	tunein.player	http://tunein.com/policies/privacy/	N/A
Yle Areena	com.yle.webtv	https://yle.fi/aihe/yleisradio/toimintaperiaatteet	Entertainment
GoodFM: Audiobook & Novels	com.newreading.goodfm	https://www.goodfm.com/terms/privacy_policy.html	Books & Reference
RadioApp – FM, AM, DAB+	au.com.radioapp	N/A (no data collected)	Music & Audio
Audials Play: Radio & Podcasts	com.audials	https://audials.com/en/privacy/android	Music & Audio
Sybel - Your favorite podcasts	co.sybel.android	https://www.sybel.co/fr/cgu/	Music & Audio
Storytel: Audiobooks & Ebooks	grit.storytel.app	https://www.storytel.com/privacy-policy	Books & Reference
Anghami: Play music & Podcasts	com.anghami	https://www.anghami.com/legal	Music & Audio
Polestar Space Warp	com.polestar.spacewarp.production.android	https://legal.polestar.com/uk/privacy/f2bfd98d7c84abc5c0a801514bc82f50	Auto & Vehicles
Polestar Performance	com.polestar.p2performancepack.production.android	N/A (no data collected)	Auto & Vehicles
Journey Log	com.polestar.driver.journey.log.production.android	https://legal.polestar.com/uk/privacy/privacy-notice-journey-log-app	Auto & Vehicles
Polestar Video Player	com.polestar.web.production.android	https://legal.polestar.com/uk/privacy/privacy-notice-video-player/	Auto & Vehicles
AccuWeather	com.polestar.accuweather.production.android	N/A (no data collected)	Weather
EVMap - EV chargers	net.vonforst.evmap	https://evmap.vonforst.net/de/privacy.html	Maps & Navigation
Radio Paradise	com.earthflare.android.radioparadisewidget.gpv2	https://legacy.radioparadise.com/#name=About&file=privacy	Music & Audio
RADIO.COM Automotive	com.radiocom.auto	N/A (no information available)	Music & Audio
Car Sounds Automotive	com.gersonlohman.carsounds	N/A (no information available)	Auto & Vehicles
L'Équipe for Renault	com.podcastslequipe	N/A (no data collected)	Sports
Radioline: Radio & Podcasts	com.radioline.android.radioline	https://www.radioline.co/privacy-policy	Music & Audio

TABLE 6 Permission analysis for dangerous protection level and indication of GDPR and CCPA compliance

Package Name	Permission Declared	LOC.	CAM.	CAL.	STORAGE	MIC.	SENSOR	CONTACTS	PERSISTENTID	GDPR	CCPA	# Discrepancies
com.polestar.abrp. production.android	Manifest	X	X	X	X	X	X			X		3
	Privacy Policy	X			X		X					
com.polestar. easypark.production. android	Manifest	X							X			0
	Privacy Policy	X							X			
com.sygic.aura	Manifest	X			X		X			X		2
	Privacy Policy	X										
com.xatori.Plugshare	Manifest	X						X		X	X	1
	Privacy Policy	X							X			
com.parkwhiz. driverApp	Manifest	X									X	0
	Privacy Policy	X										
com.coulombtech	Manifest	X									X	0
	Privacy Policy	X	X		X							
nl.flitsmeister	Manifest	X		X	X	X	X	X	X			5
	Privacy Policy	X							X			
com.spothero. spothero	Manifest	X			X			X	X		X	1
	Privacy Policy	X						X	X			
com.google.android. apps.maps	Manifest	X			X		X	X	X		X	1
	Privacy Policy	X			X		X		X			
com.polestar.driver. journey.log. production.android. apk	Manifest	X								X		0
	Privacy Policy	X										
com.polestar. spacewarp. production.android	Manifest											0
	Privacy Policy	X										
com.polestar. p2performancepack. production.android	Manifest	X							X			2
	Privacy Policy											
com.polestar.web. production.android	Manifest								X	X		0
	Privacy Policy								X			
net.vonforst.evmap	Manifest	X							X			0
	Privacy Policy	X							X			

Positions and opinions advanced in this work are those of the author(s) and not necessarily those of SAE International. Responsibility for the content of the work lies solely with the author(s).

ISSN 0148-7191