Automatic Transmission: An Empirical Study of Data Privacy in the Connected Vehicle Ecosystem

Nicole Zagson*
Northeastern University
Boston, United States
gerzon.n@northeastern.edu

Sarah Elizabeth Gillespie*
Northeastern University
Boston, United States
gillespie.s@northeastern.edu

Jason Veara
Northeastern University
Boston, United States
veara.j@northeastern.edu

Devin Patel
Northeastern University
Boston, United States
patel.devin1@northeastern.edu

David Choffnes
Northeastern University
Boston, United States
choffnes@ccs.neu.edu

Alan Mislove
Northeastern University
Boston, United States
amislove@ccs.neu.edu

Aanjhan Ranganathan
Northeastern University
Boston, United States
aanjhan.ranganathan@northeastern.edu

Piotr Sapiezynski
Northeastern University
Boston, United States
p.sapiezynski@northeastern.edu

Christo Wilson
Northeastern University
Boston, United States
c.wilson@northeastern.edu

Abstract

Modern vehicles typically integrate a wide array of sensors, software systems, and always-on connectivity, effectively becoming "smartphones on wheels." Such vehicles are part of a broader ecosystem that includes companion mobile apps and third-party services, raising significant privacy risks due to the sensitivity of vehicular data. Despite documented harms, the community still lacks a good understanding of the privacy implications of the connected vehicle ecosystem.

In this paper, we present the first large-scale empirical study of data privacy in the connected vehicle ecosystem. In collaboration with a consumer vehicle testing organization, we use two perspectives to better understand the data that is being collected and shared. First, we test 21 late model vehicles using a combination of Wi-Fi interception and controlled cellular capture under a range of conditions to observe the vehicles' network traffic patterns. Second, we instrument 30 vehicle companion apps paired with on-site vehicles to build a more complete picture of the data flows to third-party services. We find that both vehicles and companion apps contact numerous third-party domains, including advertisers and trackers. For example, all but two of the vehicles tested send traffic to at least one third party, and seven of 30 apps transmit sensitive identifiers to third-party companies, with wide variation across brands and models. Our findings underscore the need for continued measurement and scrutiny of the connected vehicle ecosystem.

*Co-first authors on this work.

IMC '26, Karlsruhe, Germany

ACM ISBN 979-8-4007-2327-8/2026/10
https://doi.org/10.1145/3777912.3839795

CCS Concepts

• **Social and professional topics** → **Consumer products policy**; **Privacy policies**; • **Security and privacy** → **Privacy protections**.

Keywords

Measurement, Vehicle Privacy, App Privacy, Network Measurement

ACM Reference Format:
Nicole Zagson, Sarah Elizabeth Gillespie, Jason Veara, Devin Patel, David Choffnes, Alan Mislove, Aanjhan Ranganathan, Piotr Sapiezynski, and Christo Wilson. 2026. Automatic Transmission: An Empirical Study of Data Privacy in the Connected Vehicle Ecosystem. In *Proceedings of the 2026 ACM Internet Measurement Conference (IMC '26), October 12–16, 2026, Karlsruhe, Germany.* ACM, New York, NY, USA, 18 pages. https://doi.org/10.1145/3777912.3839795

1 Introduction

Vehicles today are often referred to as "smartphones on wheels" [50]. The majority of new vehicles sold now feature ubiquitous Internet connectivity (Wi-Fi, cellular, and/or satellite) coupled with a diverse set of sensors (e.g., cameras, microphones, GPS receivers), rich infotainment systems, manufacturer-operated online services, and companion smartphone apps. The result is a diverse ecosystem that allows vehicle owners, vehicle manufacturers, and—in some cases—third parties to remotely control and monitor their vehicle (e.g., collecting telematics, or intervening in case of theft).

Although the connected vehicle ecosystem provides useful functionality to owners, it also raises privacy concerns due to the sensitivity of vehicular data (e.g., real-time location) and the opacity surrounding who the data is shared with. These concerns are not theoretical. In 2016, the Mozilla Foundation's review of vehicle manufacturer privacy policies described the entire category as a "privacy nightmare," finding that manufacturers routinely disclosed the potential to collect a wide variety of personal data for overbroad and opaque purposes [19]. More recent reporting revealed that multiple large vehicle manufacturers secretly share data collected from vehicles with data brokers and insurers [47–49, 58], resulting in a

U.S. Federal Trade Commission (FTC) enforcement action against General Motors [32]. Beyond commercial exploitation, connected vehicles have also raised concerns about impacts on vulnerable populations (e.g., enabling stalkers [33, 46, 99]) and U.S. national security as a whole [17].

Unfortunately, beyond the instances highlighted above, relatively little is known about the privacy implications of the connected vehicle ecosystem. Prior work has examined infotainment systems [53, 65], policy documents [12, 13], and vehicles' internal components [21, 69, 92] in isolation, but none have examined the broader ecosystem of data collection and sharing. This is in contrast to other consumer product ecosystems that collect similarly private data—such as smartphone apps [4, 26], internet-of-things (IoT) devices [77, 105], and even medical devices [43, 57]—that have been extensively studied for years.

We believe this situation is due to three key challenges that the connected vehicle ecosystem presents. First, vehicles are significantly more expensive than other consumer products; this makes it cost-prohibitive for researchers to study the connected vehicle ecosystem at scale. Second, most connected vehicles are equipped with either cellular or satellite connectivity; compared to devices that only use Wi-Fi or Bluetooth, this makes it much more difficult for researchers without privileged network access to interpose on the communication due to the protocol complexity, the lack of robust tools for network traffic capture, and the legal issues concerning licensed spectrum. Third, connected vehicles often rely on proprietary telematics control units rather than the commodity hardware and open stacks that have enabled measurement research on smartphones and IoT devices.

In this paper, we take the first steps to address the limited visibility into the privacy implications of the connected vehicle ecosystem, without requiring any privileged access to vehicle or network systems. To do so, we identify two vantage points in the ecosystem where we can gain insight into the data that connected vehicles are sharing with both manufacturers and third parties: the vehicles themselves and the mobile apps provided by manufacturers.

To measure data flows from connected vehicles themselves, we deploy several complementary techniques to interpose on the vehicles' Wi-Fi and cellular communication. While end-to-end encryption—coupled with the inability to install trusted root certificates on vehicles—prevents us from inspecting the raw traffic, we measure the endpoints, analyze the patterns of communication with those endpoints, and characterize the purpose and implications of such communication. We exercise vehicles under a number of different conditions (driving, stationary, "turned off") to see if there are notable changes in network communication.

To measure data flows from mobile apps, we set up test smartphones with the manufacturers' apps installed and instrumented for data collection. This enables us to see the remote communication endpoints as well as use monster-in-the-middle (MitM) techniques to interpose on many of the data flows, as we were able to install trusted root certificates on our test phones. This setup not only provides visibility into how and where data is shared by companion smartphone apps, but also exposes any data that is sent directly from the vehicle to external servers before it is accessed by the app.

To generalize our findings across a wide range of connected-vehicle manufacturers, makes, and models, we need access to a large set of vehicles. To achieve this, we partner with Consumer Reports, a large, non-profit U.S. consumer product testing organization that allowed us to access their purchased fleet of vehicles. Our analysis reveals a combination of vehicle-specific data-sharing patterns, as well as those that are similar to observations from prior work on smartphones and IoT devices.

Our contributions are as follows:

- Leveraging our partnership with Consumer Reports, we examine a total of 21 U.S. vehicles from 19 brands, by far the largest and most comprehensive sample of vehicles that we are aware of. If we had to procure these vehicles ourselves, it would have cost over $1.2M.
- We develop a measurement infrastructure to interpose on the Wi-Fi connectivity of these vehicles, conducting extensive stationary and in-motion tests on a test track. We observed that all of these vehicles contact at least one third party, including advertising and tracking domains.
- We procure and deploy a Faraday tent large enough to fit a vehicle inside. This allows us to block the vehicles from the cellular network to investigate if the vehicles' network traffic swaps to the Wi-Fi interface. We test 11 vehicles in this manner and find that the results vary greatly by manufacturer.
- We instrument and monitor 30 companion mobile apps paired with local vehicles. We find that seven of these transmit sensitive identifiers (e.g., VINs, emails, phone numbers, and location) to third-parties associated with advertising and tracking, and all but one of the apps measured contact multiple advertising and tracking third parties.

Our findings underscore the need for more empirical research into data selling and sharing by vehicle makers, and for increased scrutiny of modern vehicles as the sum of their interconnected systems rather than standalone consumer products. Notably, the majority of vehicles in our study run third-party software from companies such as Google and Amazon, governed by privacy policies outside manufacturer purview, thus obscuring where consumer data flows and who is accountable for it. Following an exhaustive disclosure process with each manufacturer, one explicitly changed its data collection practices in response to our findings.

The remainder of this paper is organized as follows. § 2 provides background on the connected vehicle ecosystem and overviews related work. § 3 describes our methodology for collecting data from connected vehicles and companion apps. § 4 presents our analysis of intercepting vehicles' network traffic, § 5 presents our analysis of companion apps, and § 6 examines how our findings compare to manufacturers' privacy policies. § 7 concludes.

2 Background and Related Work

While there is extensive research on the *security* of vehicle systems (e.g., CAN bus exploits [69, 92], ECU attacks [21], and remote communication vulnerabilities [66]), our focus in this paper is on *privacy* and the connected vehicle *ecosystem*: what data is shared, and with whom? We therefore provide background on and overview prior work in three areas most relevant to our study: privacy analyses of connected vehicles, IoT devices, and mobile apps. We discuss each in turn and highlight how our work advances this literature.

2.1 Connected Vehicle Privacy and Security

While journalists and advocacy groups have highlighted troubling practices in connected vehicle data sharing, academic work on this topic remains comparatively sparse. Prior research has developed taxonomies of security and privacy risks in connected vehicles [41, 70, 75] and explored the attack surfaces exposed by network connectivity, over-the-air features, and insecure infotainment apps [14, 42, 60, 74].

Some studies have examined manufacturers' privacy policies [12, 13, 19]. They found that these policies were challenging for non-experts to read, permitted extensive collection of user and vehicle data, and omitted important details about how data would be protected and used. We complement these works by measuring actual flows of vehicle data.

Aside from sensors and data connectivity, modern vehicles also feature sophisticated head units that run their own operating systems (OS) and come with pre-installed apps for navigation, music, games, etc. [80]. When developing a modern connected vehicle, manufacturers either build a custom OS in-house or partner with a tech company to incorporate their existing automotive OS (e.g., Google's Android Automotive OS) [8]. Empirical analyses of connected vehicles have so far been limited to studying the infotainment systems on these head units. Moiz and Alalfi used static analysis to identify vulnerabilities in apps installed on a vehicle's infotainment system that could leak sensitive data [65], while Jeong et al. hosted a hacking competition where participants exploited infotainment systems to exfiltrate information [53].

Our work expands on these efforts by examining data flows from entire vehicles and their companion mobile apps, not just the onboard infotainment systems. Furthermore, we investigate intentional flows of data to manufacturers and third parties, rather than surreptitious leakage. In this study, we reference the OS of a vehicle's head unit as a potential explanation for data flows to specific third-parties.

Distinct from the head unit OS built into a vehicle as described above, Apple CarPlay and Android Auto are phone-mirroring systems that project an interface from the smartphone onto a vehicle's dashboard [6]. These phone-mirroring systems have their own privacy and security risks that have been studied by prior work [63, 85, 102]. In this study, we do not examine such systems and instead interact exclusively with each vehicle's built-in OS.

2.2 IoT Privacy and Data Sharing

Connected vehicles have certain characteristics in common with many IoT devices: both are Internet-connected devices equipped with a wide range of sensors that collect sensitive information, interact with online services, and offer companion smartphone apps while providing consumers little visibility into or control over their operation. Extensive prior work [51, 68, 77, 84] on IoT privacy analysis informs our approach to studying connected vehicles.

For example, Ren et al. [77] examined information exposure in IoT devices, focusing on traffic destinations and the inference of device activities from traffic. We use a similar method, with similar limitations: we cannot modify vehicle software and thus cannot decrypt all encrypted flows.

Wireless privacy research demonstrates that even with encrypted transmissions, metadata such as packet lengths, timing, and frequency can enable inference of occupancy, device types, and user activities in smart environments [1, 3, 40, 104]. Other studies identify threats such as user tracking, traffic fingerprinting, and eavesdropping [29, 56, 59]. Given these risks, evaluating the privacy of connected vehicles' wireless interfaces is critical, as these interfaces are the point where data leaves the vehicle.

A further lesson from the IoT and mobile ecosystem is that privacy policies do not always align with actual device behavior. Studies have identified both false negatives (i.e., devices collecting *more* data than disclosed) and false positives [89, 106, 107]. This policy/practice divergence motivates empirical measurements of connected vehicles and their companion apps, since privacy risks cannot be reliably assessed through policy analysis alone.

2.3 Mobile App Privacy and Data Sharing

To analyze vehicle companion apps, we re-use and extend techniques that have examined mobile apps [11, 35, 72]. Such studies have found pervasive exposure of personal data to first- and third-parties, in general [76, 78, 79] and in specific contexts such as children's apps [31, 81], gig work platforms [73], and mobility apps [100].

Prior work has not explored data sharing from a large set of connected-vehicle companion apps linked to real vehicles, as done in this work. Yang et al. [103] performed static analysis of vehicle Android apps and found evidence of sensitive data transmission, but did not test in conjunction with actual vehicles. Thus, by working with Consumer Reports, our work is the first to shed light on the privacy implications of manufacturers' mobile apps as used in practice.

3 Datasets and Methods

We now turn to overview the goals of our study, the datasets we collect, and the methods by which we do such collection.

3.1 Study Scope and Datasets

Overall, we aim to study the connected vehicle ecosystem to answer two key questions: *First*, what data can we observe connected vehicles and their companion apps sharing about their users, particularly personally identifiable information (PII) and sensitive data linked to PII (e.g., location)? *Second*, who receives connected vehicle data, whether directly from the vehicle or from companion smartphone apps, particularly when it comes to third parties? Is this data being transmitted to international destinations outside the U.S.?

To answer these questions, we leverage our relationship with Consumer Reports, a large U.S. non-profit organization that tests consumer vehicles. Consumer Reports will typically purchase vehicles, test them at their facility for a period ranging from weeks to months, and then sell the vehicles once they have completed testing. Consumer Reports tests recent model year vehicles from major manufacturers, including mass-market and luxury brands.

Working with Consumer Reports presented a unique opportunity to study the privacy of connected vehicles. However, doing so required our methodology to be opportunistic: we could only test

Manufacturer	Brand	Year	Model	Features		Vehicle Tests				Google Features		OS Citations
				Wi-Fi	EV	Driving	Idle	In-Tent	Cellular	AAOS	GAS	
General Motors (GM)	Buick	2024	Envista	✓	✓	✓	✓					[15, 16]
	Cadillac	2024	Lyriq	✓	✓	✓	✓	✓		✓	✓	[18, 98]
	Chevrolet	2024	Blazer	✓	✓	✓	✓	✓		✓	✓	[38]
Stellantis	Dodge	2023	Hornet	✓			✓			✓		[30, 88]
	Fiat	2024	500e	✓	✓	✓	✓	✓		✓		[28, 30]
	RAM	2025	1500 Bighorn	✓		✓	✓			✓		[30, 71]
Fisker	Fisker	2023	Ocean	✓	✓	✓	✓					[44]
Ford Motor Co.	Ford	2022	F150 Lightning	✓	✓	✓	✓					[9, 45]
	Ford	2024	Mustang GT Fastback	✓		✓	✓					[45, 86]
Honda Motor Co.	Honda	2024	Prologue Touring AWD	✓	✓	✓	✓	✓		✓	✓	[39]
Tata Motors	Land Rover	2023	Range Rover Sport	✓		✓	✓					[24, 91]
Toyota Motor Corp.	Lexus	2024	NX450H+ PHEV	✓		✓	✓					[20, 61]
	Toyota	2023	Corolla Cross	✓		✓	✓					[97]
	Subaru	2023	Solterra	✓	✓	✓	✓	✓				[96, 108]
Lucid	Lucid	2023	Air Touring	✓	✓	✓	✓	✓		✓		[55]
Mercedes-Benz Group AG	Mercedes	2023	EQS450 4Matic	✓	✓	✓	✓					[25, 64]
Renault-Nissan-Mitsubishi Alliance	Nissan	2023	Ariya Platinum	✓	✓	✓	✓	✓				[67]
Rivian	Rivian	2022	R1S	✓	✓	✓	✓	✓		✓		[90]
Tesla	Tesla	2024	Cybertruck	✓	✓	✓	✓	✓				[93]
	Tesla	2024	Model 3	✓	✓	✓	✓	✓	✓			[93]
Zhejiang Geely Holding Group	Volvo	2024	C40	✓	✓	✓	✓	✓		✓	✓	[101]

Table 1: All vehicles that we tested for this paper. We conducted stationary and driving tests with vehicles that supported Wi-Fi as well as cellular interception for the Tesla Model 3. Additionally, we tested the subset of EVs with Wi-Fi inside a Faraday tent. The Google Features columns denote which vehicles in our study implemented Android Automotive OS (AAOS) and/or Google Automotive Services (GAS).

the vehicles that Consumer Reports happened to have at their facility during our visits. Further, our testing spanned a number of visits to Consumer Reports, and vehicles that were available on earlier visits were not necessarily available on subsequent visits.

We divided our testing into two phases. In *phase 1* we focused on the vehicles, aiming to understand their patterns of communication. We first surveyed the vehicles available at Consumer Reports that offered Wi-Fi, which would allow us to connect the vehicle to our access point and interpose on the Wi-Fi communication. We identified 21 unique vehicles that met this requirement, and for each vehicle we conducted a standard suite of actions with the vehicle while also collecting the Wi-Fi traffic. For one of these Wi-Fi equipped vehicles, we were able to insert a custom SIM card into the vehicle, which allowed us to interpose on the cellular connectivity as well. To block cellular communication for the remaining vehicles, we placed 11 of the 21 Wi-Fi-equipped vehicles that were electric vehicles (EVs)[1] into a Faraday tent and retested the vehicle. An overview of the vehicles we tested is available in Table 1, and § 3.2 details our methodology for collecting and examining this traffic.

In *phase 2* we focused on the companion mobile apps that manufacturers provide to owners to remotely access and control their vehicle. We first surveyed the vehicles available at Consumer Reports that offered companion apps that we could install on our instrumented smartphones. We identified a total of 32 vehicles that used 30 unique mobile apps (some manufacturers use the same app for multiple makes/models) for testing.[2] To analyze each app, we installed it on a test device, logged-in to a valid user account tied to one of Consumer Reports's vehicles, exercised all in-app functionality, and captured the app's network traffic. An overview of the apps we tested is available in Table 2, and § 3.3 details our methodology for collecting and examining traffic from apps.

Figure 1 presents the scope of the ecosystem that we focus on in this work. By examining a vehicle and its companion mobile app we are able to see the first layer of data flows that may expose consumers to privacy risks.

3.2 Data Collection from Vehicles

Recall that in the first phase of our testing, we focused on vehicles' Wi-Fi and cellular Internet connectivity to understand the communication patterns of the vehicles themselves. For each vehicle that supported Wi-Fi, we captured traffic under a range of conditions. For cellular, we either blocked connectivity or, in one case, directly intercepted traffic.

3.2.1 Wi-Fi Traffic Capture. To collect Wi-Fi traffic from vehicles, we configured a custom access point (AP) on a Raspberry Pi and used `tcpdump` to log all packets that were sent or received via this AP. The Raspberry Pi was configured with an Internet connection either from Ethernet or a mobile hotspot, and was configured to forward traffic received by the AP to the intended destination after

[1]We tested only EVs in the tent to avoid the known hazards of running combustion engines in an enclosed, poorly ventilated space.

[2]Due to the timeline of our testing, these vehicles only partially overlap with the vehicles tested in phase 1.

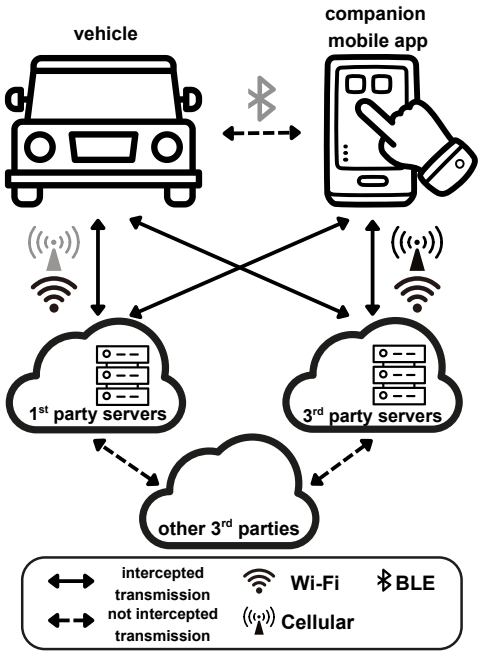

Figure 1: Diagram depicting the potential data flows to and from a vehicle and its companion mobile app. Solid arrows represent flows that were intercepted through our experiments.

logging. We then connected each of the 21 vehicles that supported Wi-Fi[3] to this AP, ensuring that the AP was positioned near the vehicle at all times to ensure reliable connectivity. We tested each vehicle under three conditions:

1. Stationary Idle: The vehicle was powered on, parked, and left untouched for 30 minutes. This established the baseline level of traffic when the vehicle was idle.

2. Stationary Active: The vehicle was parked and powered on for 30 minutes while we interacted with as many sensors and features as possible. This included opening and closing doors and the trunk, pressing dashboard and seat controls, activating stalks (lights, wipers), and exploring all infotainment menus and apps.

3. Driving: The vehicle was driven on private roads at Consumer Reports's facility for 15 minutes at moderate speeds (5–45 mph), with bursts of acceleration, hard braking, and swerving to safely emulate reckless driving.[4]

The vast majority of traffic we captured from vehicles over Wi-Fi was HTTP traffic encrypted with TLS. We unsuccessfully explored two approaches to gain visibility into payload contents: (i) installing custom root certificates into the vehicles' trust stores, which would have required destructive modifications that were not permitted by Consumer Reports, and (ii) injecting modified certificates during TLS handshakes using monster-in-the-middle (MitM) techniques,

[3]Note that some connected vehicles can also establish Wi-Fi hot spots. We did not test this functionality in our experiments.

[4]All driving tests were conducted on private roads within Consumer Reports's gated and fenced test facility to ensure safety and consistency across experiments.

Figure 2: We drove the vehicles into this Faraday tent to block external cellular signals.

which were correctly rejected by all tested vehicles as the corresponding root certificate was not trusted by the vehicles. These results show that manufacturers are enforcing certificate validation.

Although payloads remained opaque to us, the network traces still yielded valuable information, including the domains contacted via DNS traffic, Server Name Indication (SNI) in TLS handshakes, the volume and timing of transmissions, and differences in behavior across experimental scenarios. This is consistent with other work that has been unable to decrypt traffic but gained insights from traffic patterns [7, 77, 87].

3.2.2 Cellular Traffic Isolation and Capture. All vehicles in Table 1 included an active cellular connection by default.[5] When both Wi-Fi and cellular are enabled, vehicles may transmit data over either interface, creating a challenge for our study. With one exception, described below, we were unable to intercept the cellular traffic from the vehicles in our sample because they were configured to use eSIMs provisioned by the manufacturer. While it is theoretically possible to load a custom eSIM on some vehicles, there is no reliable way to restore the factory configuration afterwards, and Consumer Reports did not permit us to make potentially destructive modifications to vehicles. To address these limitations, we used two complementary strategies described below:

1. Forcing Wi-Fi Traffic: One hypothesis we tested was whether blocking a vehicle's ability to communicate over its cellular network would force more Wi-Fi communication. To block external cellular signals, we placed each of the 11 vehicles that supported Wi-Fi and were EVs inside a professionally constructed 5.8 m × 2.75 m × 2.45 m Faraday tent (see Figure 2), which provided ≈93 dB attenuation across cellular frequencies. For each of these EVs, we performed the Stationary Idle and Stationary Active tests inside the tent (see Table 1); unfortunately, the Faraday tent was not large enough to enable the Driving tests.

2. Intercepting Cellular Traffic: The 2024 Tesla Model 3 was unique among the tested EVs in that it (a) contains a physical SIM card slot, (b) that is user-accessible, and (c) there is documentation online that describes how to force the vehicle to use the

[5]Consumer Reports did not purchase optional upgraded "online" packages; the Wi-Fi and cellular functionality we tested reflects the standard configuration.

Manufacturer	Brand	App Name	Version
BMW	BMW	My BMW	5.3.0
	Mini Cooper	MINI	5.3.3
mfgcol	Chrysler	Chrysler	1.98.1
mfgcol	Fiat	FIAT	1.98.1
mfgcol Stellantis	Jeep	Jeep	1.98.1
mfgcol	Maserati	Maserati Connect North America	1.98.1
mfgcol	RAM	RAM	1.98.1
Ford Motor Co.	Ford	FordPass	5.6.0
	Lincoln	Lincoln	5.15.0
General Motors (GM)	GMC	GMC	7.4.1
	Buick	myBuick	7.4.0
	Cadillac	myCadillac	7.3.3
	Chevrolet	myChevrolet	7.4.0
mfgcol Honda Motor Co.	Honda	HondaLink	5.0.25
mfgcol	Hyundai	MyHyundai with Bluelink	5.2.8
mfgcol Hyundai Motor Group	Genesis	GenesisIA	3.2.0
mfgcol	Kia	KiaAccess	7.12.0
mfgcol Tata Motors	Land Rover	Land Rover Remote	3.0.0
mfgcol	Lexus	Lexus	2.5.7
mfgcol Toyota Motor Corp.	Subaru Solterra	Subaru Solterra Connect	1.0.14
mfgcol	Toyota	Toyota	2.5.7
mfgcol Lucid	Lucid	Lucid	2.2.0
mfgcol Mazda	Mazda	MyMazda	8.7.3
mfgcol Daimler AG	Mercedes	Mercedes-Benz	3.53.3
mfgcol Renault-Nissan-Mitsubishi Alliance	Nissan	MyNISSAN	6.3.67
mfgcol Rivian	Rivian	Rivian	2.17.0
mfgcol Subaru Corp.	Subaru	MySubaru	3.1.2
mfgcol Tesla	Tesla	Tesla	4.42.5
mfgcol Volkswagen Group	Volkswagen	myVW	2025.2.1
mfgcol Zhejiang Geely Holding Group	Volvo	Volvo Cars	5.52.0

Table 2: Companion mobile apps we investigated, broken down by manufacturer, brand, and specific app and version we tested.

user-provided SIM over the provisioned eSIM. These features together allowed us to implement controlled cellular interception for this vehicle. While this measurement cannot be generalized to other vehicle make/models due to their lack of a physical SIM slot, it shows a proof-of-concept for intercepting cellular traffic from modern vehicles, which may be extended to eSIMs in the future. We achieved this by using a custom-programmed sysmocom SIM card (sysmoISIM-SJA5-S17) with T-Mobile credentials. The SIM was created using `pySIM` and installed and activated following Tesla's documented service procedures [94]. We then emulated a local LTE/5G network with an Amarisoft AMARI Callbox Classic [5]. To comply with U.S. Federal Communications Commission (FCC) rules governing the use of licensed spectrum, we only used this setup inside the Faraday tent to avoid interference with external devices.

As with the Wi-Fi capture described above, this process allowed us to view the traffic transmitted by the vehicle but not decrypt application-level traffic (e.g., TLS).

3.3 Data Collection from Companion Apps

Much like IoT devices, many modern vehicles include companion mobile apps. In total, we experimented with 30 connected vehicle companion apps (see Table 2) that were paired with the vehicles at Consumer Reports's testing facility.

To exercise each app, we installed it on a test smartphone and then had a Consumer Reports employee log into the app using their existing credentials associated with a vehicle on the lot. This approach enabled us to engage with the full functionality of each app, except for the initial account setup process. During app installation and login we accepted all permission requests (e.g., tracking, location, calendar access, Bluetooth, notifications) that the application requested. Once we were logged-in, we manually exercised all available functionality, such as looking for nearby charging stations, geolocating the vehicle, viewing vehicle data and service history (e.g., tire pressure), viewing notifications (e.g., "doors are unlocked"), and viewing in-app privacy policies. Some apps allowed us to perform physical interactions on the vehicle, such as remotely opening the trunk. We performed all such actions and verified that the vehicle completed each request.

We used a combination of test phones and iOS versions for our experiments: an iPhone 8/iOS 16.6, an iPhone X/iOS 16.7.11, and an iPhone 13/iOS 18.5. To minimize background traffic, we deleted all non-essential apps on the test phones and tested apps one-by-one, including deleting each vehicle app and restarting the phone before downloading the next app. We used the iOS native screen recording feature to record our interactions with each app for later review.

To capture and decrypt network traffic from the companion mobile apps, we used iPhones with custom root certificates connected to `mitmproxy` [22]. We observed that some companion apps performed certificate pinning on domains that were critical for user account authentication; we used `mitmproxy`'s "ignore hosts" option to avoid interception to these domains. Table A2 in the Appendix lists the domain patterns we did not intercept for MitM analysis; as can be observed, the vast majority of these domains were first-party (i.e., manufacturer) domains.

3.4 Traffic Analysis Methodology

As described above, we collected network traffic traces from vehicles and their companion mobile apps. Using this data, we aim to answer three different classes of questions: who received what data, where was data sent geographically, and did vehicles' network traffic change under different experimental conditions?

3.4.1 Classifying Domain Names. To answer questions related to the destinations of vehicle traffic, we extracted domain names from DNS requests as well as Server Name Indication (SNI) fields in TLS handshakes. We manually reviewed each effective second level domain (SLD) that appeared in our traces using WHOIS to determine if it was a first-party (manufacturer) or third-party domain.

We note that many manufacturers' domains include the name of the manufacturer or their vehicle brand, while others referred to parent companies. For example, we labeled flows to *gm.com*, *gm-cdn.com*, *cadillac.com*, *buick.com*, *chevrolet.com*, and *gmc.com* as first party if they originated from a GM vehicle or a GM companion mobile app. In other cases, we were able to determine through a manual online search that specific domains belonged to wholly-owned subsidiaries of specific manufacturers. For example, *autonomic.ai* belongs to a vehicle cloud provider that was purchased by Ford in 2023. There were also notable exceptions, such as the Subaru Solterra, whose internals were developed by Toyota, and the Honda Prologue, which was co-developed with GM. For these vehicles we treated both manufacturers as first parties.

Using WHOIS, TLS certificate ownership, and manual online search of registered domain info and company names, we manually

classified third-party domains into four categories: *support*, *integrated*, *advertising/tracker/analytics* (*ATA*) and *other*. The *support* category includes content delivery networks, cloud providers, and other network infrastructure. The *integrated* category encompassed third parties that are integrated into vehicle infotainment systems. Examples include navigation (e.g., *tomtom.com*, *here.com*), roadside assistance (e.g., *aaa.com*, *tweddle.io*), preinstalled apps (e.g., *tiktok.com*, *youtube.com*), and OS-level services (e.g., Google's AI Assistant for Android Auto).

We found that we could not easily re-use existing lists of ATA domains. For example, the EasyList and EasyPrivacy blocklists along with the Disconnect and App X-Ray databases are often used in prior work to identify ATA domains [10, 34, 54, 76]. However, we found false positives and false negatives when we applied them to our traffic traces as these lists misclassified 360 (26.91%) fully-qualified domain names (FQDNs) in our full dataset. False negatives arose from vehicle-specific ATA domains that have not been observed on the web—the primary target of our custom lists. False positives arose from domains that are rightly classified as ATA when they appear as third parties on the web, but are legitimate traffic destinations in the connected vehicle context (e.g., first party domains such as *mazda.com*), as well as third parties that we classify as integrated due to their purposeful inclusion within the vehicle's head unit or companion mobile app.

Out of 1,338 unique FQDNs that appeared in our data, we classified 227 as *first party*, 136 as *support*, 600 as *integrated*, and 367 as *ATA*. Two authors manually reviewed all third-party domains and independently classified them. Then the labelers met and discussed all FQDNs with conflicting labels until there was full agreement. In the case of 8 FQDNs, the labelers were unable to find sufficient information to reach full agreement on their categorization, thus we label them as *other* third parties.[6]

3.4.2 IP Address Geolocation. Since we experimented with U.S. vehicles that were physically located in the U.S., we explored whether our test vehicles or mobile apps contacted destinations that were outside the U.S. This is of particular interest, given the recent focus of U.S. federal agencies on the potential threats posed by foreign-made connected vehicles [17]. Further, data transfers that cross jurisdictions may invoke conflicting—and potentially more stringent—consumer data regulations.

We used IPinfo's Researcher API [52] to request the location data for all of the destination IP addresses that appeared in our traffic traces. We adopted an approach modeled off of Gamero-Garrido et al. [36] to validate IPinfo geolocation data including collecting additional metadata for the IP addresses from RIPE Atlas Probe pings, traceroutes [82], and reverse DNS lookups as well as WHOIS information, DNS records, and data from the CAIDA Hoiho API [62] from all domain names that were associated with these IP addresses.

Using this methodology, we find multiple instances of vehicles and apps contacting first and third party servers located in the EU and Canada, which have stricter consumer data regulations than the US. Table A1 presents the full table of international IP addresses observed in our study.

3.4.3 Comparing Network Destinations. Changing experiment conditions may cause vehicles to change their behavior at the network level. Thus, we analyze differences in the destinations contacted in each experimental scenario. For this analysis, we use Jaccard similarity and set size difference between the sets of SLDs contacted under different test conditions. In our analysis, a Jaccard similarity of 1 means the two experiments contact the exact same set of SLDs, whereas 0 indicates that the set of SLDs contacted is disjoint. In cases where the similarity is less than 1, we also use set size difference, to understand whether a vehicle contacted more or less domains in two different conditions; positive set size differences imply more SLDs were contacted in the first condition, and vice versa for negative differences.

3.5 Limitations

We investigated 21 vehicles from the U.S. market in a controlled environment along with 30 companion mobile apps instrumented with on-site vehicles between October 2024 and August 2025. While we tested a wide range of vehicles, we did not cover every manufacturer in the U.S. market. As with all empirical studies, our results should be interpreted as a snapshot in time, and may not generalize to vehicles outside our sample or outside the U.S.

Our visibility into the contents of network flows is limited in two ways: we could not decrypt the content of traffic sent by vehicles and we could not decrypt mobile app traffic to a subset of first-party destinations that were protected by TLS certificate pinning. For this reason, the analysis we present in § 5 should be considered a *lower bound* on privacy risks and violations.

In addition, we were unable to observe the cellular traffic transmitted by vehicles (except the Tesla Model 3). We present a mitigation to this limitation in § 3.2.2 by blocking the cellular transmission of EVs within our dataset using a Faraday tent. Our results in § 4.2 indicate that several vehicles in our sample route traffic to Wi-Fi when their cellular interface was blocked. However, there is no guarantee that those vehicles redirected *all* of their traffic to the Wi-Fi interface or that other vehicles would not exhibit different behaviors. Future work may be able to overcome this limitation by reprogramming vehicles' eSIMs.

Finally, there may be server-side flows of data from vehicle makers to third parties that are unobservable from our vantage points. Thus, the communication patterns we observe should be considered a lower bound on the set of third parties information is shared with.

4 Vehicle Communication Analysis

In this section, we present analysis of the network traffic we collected from vehicles. We answer the following key questions:

(1) How many destinations are contacted per vehicle? (§ 4.1.1, Table 4)
(2) What is the purpose of the entities associated with these destinations? (§ 4.1.1, § 4.1.2)
(3) How do data flows to third parties vary across vehicles? (§ 4.1.2, § 4.2, Table 3)
(4) How do data flows from vehicles vary under different experimental scenarios? (§ 4.2, Figure 4)

[6]The full lists used to label ATA, integrated, and first party domains can be accessed at https://github.com/nicolegerzon813/Automatic-Transmission-An-Empirical-Study-of-Data-Privacy-in-the-Connected-Vehicle-Ecosystem.

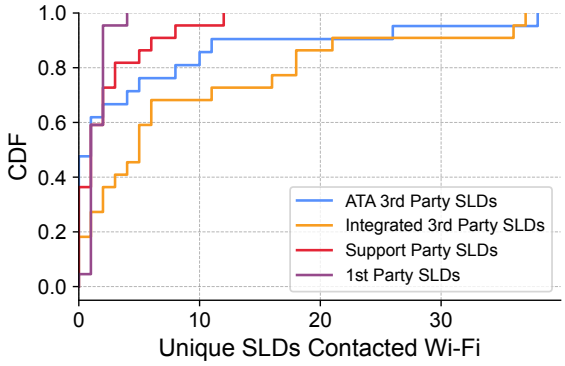

Figure 3: CDF of unique SLDs contacted by each of the tested vehicles over Wi-Fi. We plot separate lines for first party, support, integrated third party, and ads/tracking/analytics SLDs.

	Unique SLDs			
Vehicle	**ATA**	**Integrated**	**Support**	**1st Party**
Tesla Model 3	34	36	7	2
Tesla Cybertruck	23	37	4	2
Cadillac Lyriq	10	21	2	2
Lucid Air	9	15	2	4
Chevrolet Blazer	7	18	2	2
...	...	...	...	...
Toyota Corolla Cross	1	1	0	1
Nissan Ariya	0	1	1	1
Land Rover Range Rover	0	0	1	1
Mercedes EQS	0	0	0	1
Buick Envista	0	0	0	1

Table 3: The top and bottom five vehicles, sorted by count of unique ATA SLDs they contacted via Wi-Fi, broken down by category. Table A3 in the Appendix presents the full table.

4.1 Destination Analysis

We begin by analyzing the destinations that vehicles contact. For this analysis, we include all traffic traces that we gathered from the Wi-Fi interfaces of the 21 cars that supported Wi-Fi (see Table 1) across all experiment scenarios (e.g., Stationary Idle, Stationary Active, Driving, and Forcing Wi-Fi Traffic).

4.1.1 Destinations Contacted. We begin by analyzing traffic captured across all experimental scenarios. Figure 3 presents the empirical cumulative distribution function (CDF) of unique SLDs contacted per vehicle, stratified into first parties, support, integrated, and ATA-related SLDs. We observe that vehicles in our sample contacted at most four first-party SLDs each, as compared to 9.29 integrated third parties on average (median = 5). 11 vehicles contacted at least one SLD that specializes in ATA, with their mean being 8.7 unique SLDs per vehicle (median = 5). Figure 3 shows that, in most cases, ATA SLDs were more common than support parties, but less common than integrated third parties.

Table 3 presents details for the top and bottom five vehicles, sorted by unique ATA-related SLDs contacted (second column). Many of the vehicles in our dataset share similar OS developers (e.g., Google, see Table 1) and we observe a relationship between OS and the third parties contacted by the vehicle. For example, vehicles with sophisticated infotainment systems (Tesla Model 3 & Cybertruck, Lucid Air, Rivian R1S), along with those that implemented full Android Automotive with built-in Google Automotive Services (Chevrolet Blazer, Cadillac Lyriq) contacted the most ATA and integrated third parties. In stark contrast, vehicles like the Buick Envista, Mercedes EQS, and Land Rover Range Rover had relatively limited functionality in their infotainment systems and only contacted one or two unique SLDs each.

Surprisingly, our results show that vehicles belonging to related brands may exhibit different behaviors. The Buick Envista, a notable outlier, shares the same backend manufacturer as the Cadillac Lyriq and the Chevrolet Blazer, but does not implement AAOS or GAS (see Table 1), which is likely the reason it contacts far fewer SLDs in general. These observations highlight the breadth of Internet-enabled behaviors exhibited by the vehicles in our sample, with some functioning more like smartphones that contact many parties, and others operating more like limited-purpose appliances.

4.1.2 Common Third Parties. Table 4 presents the top third-party companies that the vehicles in our sample contacted over Wi-Fi, sorted by the number of unique vehicles that contacted each third-party. We also present the category of unique SLDs (see § 3.4.1) associated with each third party. We observe vehicles contacting large technology companies, including Alphabet (Google), Amazon, Microsoft, and Meta. Of the 21 vehicles we tested, 13 contacted Google-associated ATA SLDs. Several of these vehicles' infotainment systems were implemented using Google's Android Automotive OS (see Table 1), but many of the SLDs we observed were not necessary for core services (e.g., *doubleclick.net* and *googlesyndication.com*, which are used for advertising purposes).

Other companies in Table 4 can be service providers in the vehicle context: Spotify and Liberty Media Corporation (SiriusXM's parent company) stream audio, while TomTom, Mapbox, and HERE provide maps and navigation. Spotify and Liberty Media are notable cases in that their SLDs may provide media and also collect tracking

		Unique SLDs		
Company Name	**Vehicles**	**ATA**	**Integrated**	**Support**
Alphabet Inc	13	11	12	1
Amazon	12	3	7	5
Spotify	8	3	4	0
Liberty Media Corporation	7	0	1	0
Cloudflare, Inc	6	0	1	2
Microsoft	6	2	2	5
TomTom International B.V.	5	0	1	0
HERE Global B.V.	4	0	2	0
Mapbox	4	0	1	0
Meta Platforms, Inc.	3	2	0	0

Table 4: The top 10 third-party companies contacted by vehicles in our sample over Wi-Fi, sorted by count of unique vehicles. We also present the total and unique number of SLDs associated with each company along with their categories (ATA, integrated, support). Table A5 in the Appendix presents the full table.

data for behavioral ad targeting. In these cases, we distinguished between integrated and ATA use cases by examining full FQDNs.

As we discussed in § 2, connected vehicles resemble both mobile apps and IoT devices in terms of capabilities. To understand how this dual role manifests in Wi-Fi traffic, we compare ATA destinations we classify to those identified by EasyList, EasyPrivacy, Disconnect, and App X-Ray databases. Out of 113 unique ATA FQDNs contacted by vehicles in our sample, 99 of these were correctly identified as ATA by off-the-shelf detection lists. For example, popularly contacted domains such as *ad.doubleclick.net*, *sb.scorecardresearch.com*, and *graph.facebook.com* were correctly classified. However, these lists incorrectly flagged 190 non-ATA domains, demonstrating their overly broad definition of ATA when applied to vehicles. For example, *api.mapbox.com* and *android.google-apis.com* were both classified as ATA domains, but serve core functionality in vehicles as maps and the Android OS backend, respectively. Our custom approach also revealed 14 vehicle-focused ATA FQDNs that were missed by ATA lists and prior work, such as *appsvc-ingest.inrix.io*.

Key Takeaways

1. Connected vehicles contact well-known trackers as well as vehicle-specific ATA domains not seen in prior work.
2. The number and types of domains contacted by connected vehicles varies greatly by manufacturer, and even within the same brand.

4.2 Variation by Experimental Scenario

In § 3.2.1 and § 3.2.2, we described the different experimental scenarios for testing vehicles. Recall that the design of these experiments is intended to test the following hypotheses:

Stationary Idle vs. Stationary Active: We expect that vehicles will send more data to and contact more unique destinations while their infotainment units and other functionality are tested, compared to idle experiments.

Stationary Idle vs. Driving: Given reports of driving behavior being reported to data brokers and insurance companies [47], we expect that vehicles may report more data when they are in motion or when driven recklessly.

In Tent vs. Out of Tent: We hypothesize that when vehicles lose access to the cellular network they will reroute traffic to our instrumented Wi-Fi connection, resulting in more traffic observed and new domains contacted within the tent.

To test our hypotheses, we present analysis below to identify significant differences in communication patterns for the same vehicle in different scenarios. Figure 4 presents comparisons between each of these experimental hypotheses using the metrics introduced in § 3.4.3, separated by column per experiment. The top row of figures depict the CDF of the Jaccard similarity metric for the sets of domains contacted by each vehicle, whereas the bottom figures depict the CDF of set size differences. In each case we present separate comparisons between the sets of first party, support, integrated third party, and ATA domains.

4.2.1 Stationary Active vs. Stationary Idle. Focusing on the leftmost column of Figure 4, we observe that at least half of the vehicles contact the exact same domains (i.e., Jaccard similarity is 1) in both stationary active and idle scenarios. The SLDs that are least likely to change are first party, which makes sense given that first-party communication is likely providing always-on functionality like remote start. However, we see that third-party SLDs tell a different story, with vehicles exhibiting bimodal behavior: some demonstrate little change between active and idle (top right of the top figure), while others see substantial differences (bottom left).

A key question is whether these changes in destinations are mainly due to new domains being contacted in active experiments, or domains no longer being contacted. The most common behavior is zero set size difference, explaining the common case where the Jaccard similarity is 1. For the remaining cases, all but two vehicles contacted *more* domains during active experiments than idle. This confirms our hypothesis that, in some instances, active experiments are causing vehicles to contact more domains. The Cadillac Lyriq, Tesla Cybertruck, Lucid Air, and Tesla Model 3 see the largest increases in ATA domains, while the Rivian R1S and Fisker Ocean are the only ones with fewer tracking domains while active.

4.2.2 Stationary Idle vs. Driving. During our testing, we found that several vehicles (Land Rover, Mercedes, Nissan) automatically turned off Wi-Fi when we shifted out of "Park" or the vehicle was in motion for a few moments. These vehicles necessarily have less communication over Wi-Fi than those that keep the connection alive. Other vehicles, such as the Tesla Model 3 and Cybertruck, have a non-default option to keep Wi-Fi on while driving, which we turned on to maximize the data available to us.

We see these trends of decreased Wi-Fi traffic when driving in the second column of Figure 4, where we compare the driving and stationary idle experiments. We find that over half of the vehicles contact the same set of domains and, in general, there is a decrease in traffic and domains contacted while driving. In fact, comparing this column to the first column of Figure 4 reveals more similarities between driving and stationary idle experiments than seen when comparing idle and active stationary experiments. This implies that there is less communication with third parties—and ATA—while driving than while using the infotainment systems. One notable exception is the Tesla Cybertruck, which contacts 19 more integrated third-party domains—and seven more ATA domains—while driving than while stationary.

4.2.3 Inside versus Outside the Tent. For the next two sets of comparisons, we analyze behavior while vehicles were in the Faraday tent. Given that it was safe to do such tests only for EVs, the number of vehicles tested in this scenario is 11, compared to the 21 outside the tent. The third and fourth columns of Figure 4 show how Stationary Idle and Stationary Active traffic changes when inside versus outside the Faraday tent, respectively.

When analyzing the set size differences, we see bimodal behavior. We find that a substantial number of integrated third parties and ATA domains appear in the tent but not outside, which is likely due to the vehicle rerouting traffic from the cellular interface to Wi-Fi. We also observe the opposite effect in some cases: fewer domains contacted in the tent. While counterintuitive, we hypothesize that some vehicles may have telematics systems that bootstrap over the cellular connection. Thus, when cellular is unavailable, subsystems within these vehicles shut down entirely. Vehicles in this category

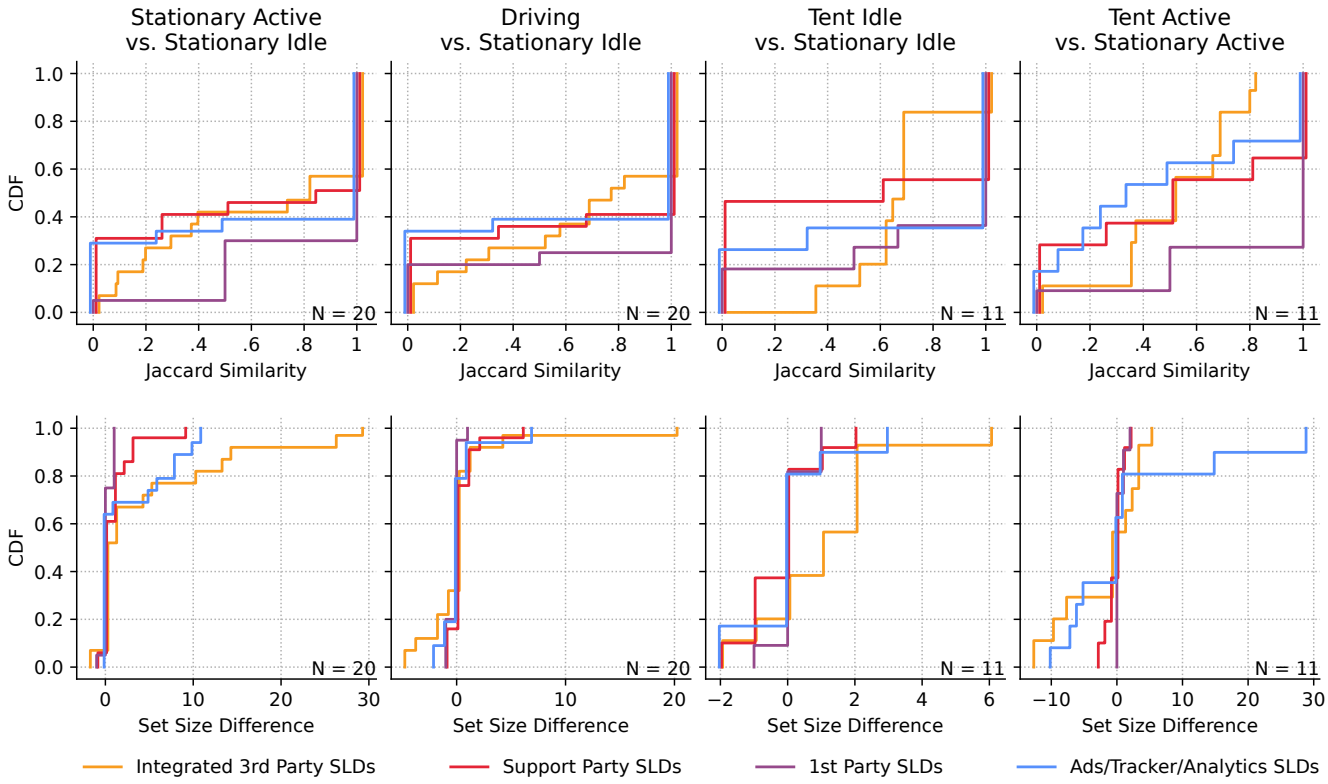

Figure 4: Comparison of SLDs contacted by vehicles across different experimental conditions. Each column compares two experimental conditions, as labeled at the top. Top row: CDF of Jaccard similarity coefficients, measuring the overlap between domain sets contacted by each vehicle across conditions. Bottom row: CDF of the difference in set sizes, showing how the number of domains contacted changed between conditions for each vehicle. Each plot displays separate lines for first party, support, integrated third party, ads/tracking/analytics domains. N indicates the number of vehicles analyzed in each comparison.

include the Chevrolet Blazer, Rivian R1S, Cadillac Lyriq, and Honda Prologue.

While the tent does not uniformly lead to more traffic being sent over Wi-Fi, we find that for seven out of the 11 vehicles, the tent reveals more first and third parties (and particularly more ATA services) than observing Wi-Fi alone. For example, there are 27 more ATA domains for the Tesla Model 3 and 14 more for the Tesla Cybertruck, inside the tent than outside. Thus, blocking cellular communication using the tent improved visibility and underscores the complexity of accurately measuring vehicles' privacy footprints.

4.2.4 Case Study: Cellular Traffic. The previous section presented evidence that in some cases when cellular traffic was blocked by the tent we observed additional traffic diverted to the active Wi-Fi connection. To investigate if the blocking of cellular resulted in diversion to the Wi-Fi interface, we compared the set of destinations contacted by the Tesla Model 3 when it had connectivity only with Wi-Fi, only with cellular, or with both interfaces. Recall from § 3.2.2 that the Tesla Model 3 was the only vehicle that we were able to intercept cellular traffic due to it having a user-accessible SIM slot.

Using the data from our idle test scenario, we confirm that the set of destinations we observed when the vehicle had access to working cellular and Wi-Fi connections was the same as when the cellular connection was blocked. In comparison, network traffic we captured from the Model 3 outside the tent (where we interposed on Wi-Fi but did not block—and could not see—the cellular traffic) never included one domain, *conviva.com*, a domain associated with analytics and tracking. This domain appeared only over the cellular interface when we intercepted both cellular and Wi-Fi traffic inside the tent, and moved to the Wi-Fi interface when the cellular connection was blocked. This finding is in line with our hypothesis.

Key Takeaways

1. Vehicles, when active, tended to contact more domains overall and more ATA domains in particular, especially when infotainment functions were in use.
2. Some connected vehicles will direct traffic to Wi-Fi when cellular is blocked, which reveals flows to trackers previously unobservable outside the tent.

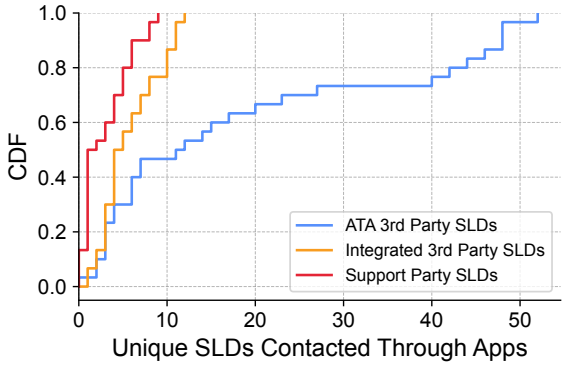

Figure 5: CDF of unique SLDs contacted by each of the companion apps. We plot separate lines for support, integrated third party, and ads/tracking/analytics SLDs.

5 Mobile App Communication Analysis

We now present analysis of the decrypted network traffic we collected from 30 companion mobile apps associated with the vehicles listed in Table 2.

5.1 Destination Analysis

We begin by analyzing the destinations that companion apps in our sample contacted. Figure 5 presents the CDF of unique SLDs contacted per companion app, stratified into support, integrated third parties, and ATA-related SLDs.[7] We observe that 70% of apps in our sample contacted more than five unique ATA SLDs, compared to only 29% of vehicles (§ 4.1).

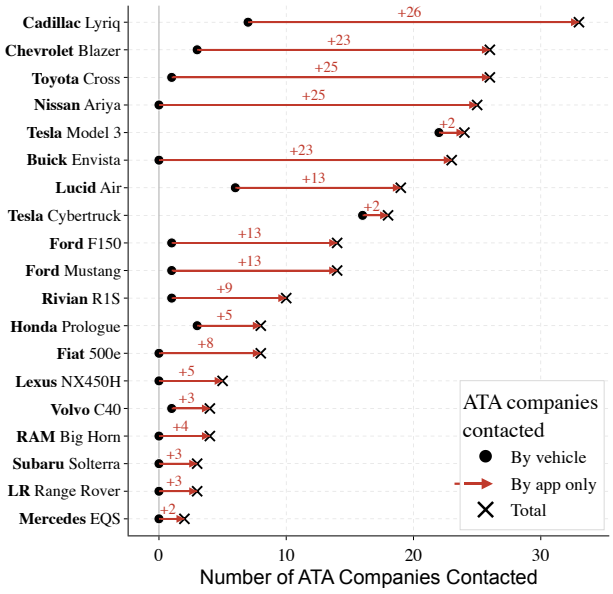

Figure 6: ATA company exposure per vehicle (•) and companion mobile app (×). Arrow labels show the count of ATA companies introduced by the companion app but absent from vehicle traffic. Vehicles sorted by total ecosystem ATA contact count ascending.

Figure 6 shows that the use of companion mobile apps substantially expand ATA exposure for the consumer beyond vehicle-only traffic. For most vehicles in our dataset, the companion app at least doubles cumulative ATA exposure; several vehicles with minimal direct ATA contact (e.g., Buick Envista, Nissan Ariya) reach 20+ ATA companies when the companion app is included. This finding underscores the necessity to evaluate vehicle privacy outcomes as a sum of the interconnected ecosystem used by the consumer, rather than just focusing on one component in isolation.

Next, we compare the ATA domains identified through our methodology to the ATA domains documented in prior work on mobile apps and IoT devices [10, 34, 54, 76]. Overall, we find a large overlap between ATA domains in these two scenarios, as well as a significant number of vehicle-specific domains that are misclassified by prior work. Unsurprisingly, companion apps contact prominent ATA companies—like Google's DoubleClick and Analytics, Facebook, and Adobe—just like other mobile apps in prior work. Out of a total of 300 unique FQDNs that we identified as ATA, existing ATA databases and blocklists correctly identified 262 of the FQDNs as tracking. Out of the 38 FQDNs that were not classified by existing lists, we find several vehicle-focused ATA domains such as *api.autointel.ai*, *b2hxak1anc.traqcliq.com*, and *cfassets.dealerinspire.com*.

ATA databases and blocklists *misclassify* 142 FQDNs as ATA when they have legitimate purposes within the companion mobile apps. Examples of these false positives include several brand-specific first-party domains (*st.mazdausa.com*, *autoparts.toyota.com*) along with destinations that service integrated functionality such as *va.v.liveperson.net* (live support chat) and *maps.googleapis.com* (built-in maps).

Key Takeaways

1. Use of vehicle companion mobile apps substantially expands consumer exposure to third party and ATA domains.
2. Companion mobile apps contact well-known trackers as well as vehicle-specific ATA domains not seen in prior work.

5.2 PII Sharing Analysis

Next, we investigate the content that companion apps transmitted to third-party SLDs, namely transmission of PII associated with the paired vehicle, driver, or app account.

To investigate transmission of PII, we manually constructed a dataset of PII associated with the accounts and vehicles used in our testing in collaboration with Consumer Reports.

The types of PII used for this analysis are listed in Table 5. We focus on PII that is vehicle specific—such as Vehicle Identification Number (VIN)[8] and license plate number—as well as types of PII

[7] Table A4 in the Appendix presents a full breakdown of app SLD contacts categorized by our taxonomy.
[8] VINs are globally-unique permanent IDs assigned to vehicles when manufactured.

Topic	Specific Data Types
Vehicle Specific	VIN, license plate number
Owner Specific	phone number, email, name
Location	latitude, longitude, home address, current address
Network Information	Wi-Fi SSID, Wi-Fi password

Table 5: PII types investigated in app traffic. Owner-specific PII corresponded to the Consumer Reports employee who completed the vehicle purchase.

that prior studies have observed third parties collecting, including location, phone numbers, and email addresses [79]. We transformed each string in our PII dataset into uppercase and lowercase versions—as well as MD5, SHA1, and SHA256 hashes—and then searched for these strings within decrypted mobile-app traffic.

Table 6 presents the seven companion apps that we observed transmitting PII to third parties, along with what they transmitted and to whom. We observe that VINs are the most commonly shared PII within our sample, including to Google, Microsoft, and Meta. We suspect that VINs are being used as stable, unique identifiers for vehicles, much like how IMEI or IDFA are used for the same purpose on smartphones (though major mobile operating systems now allow users to reset IDFA values [23], while VINs are subject to legal restrictions and cannot be changed).

We observe that vehicle-specific information is being tied to individual consumers. While a vehicle's VIN is semi-public information (it is visible if an observer is standing next to the windshield), it is generally not linkable to an individual by onlookers, nor is it exposed to ATA companies by virtue of being visible on the dashboard. In contrast, we find that companion apps expose VINs *and* another type of PII (e.g., email address) to three ATA companies (see Table 6). Such companies can use these stable identifiers and PII to implement cross-context tracking of users [2, 27], i.e., allowing advertising companies to link a person who owns a vehicle with their behavioral data and purchase history from other websites and mobile apps. Furthermore, we observe that some apps also expose detailed geolocation information to ATA companies. These transmissions expose consumers to a different level of harm than traditional mobile app tracking as they reveal an individual's ownership status or interactions with a particular vehicle to companies that use this data for advertising, tracking, and analytics.

Key Takeaways

1. Certain companion mobile apps share consumer PII with ATA third parties including geolocation, VIN, email, and phone number.
2. Sharing of VIN along with other PII allows for cross-context user tracking and exposes a new avenue of risk for consumers.

6 Manufacturer Insights

We now examine how our findings comport with manufacturers' stated privacy policies. We also disclosed our findings to all manufacturers, and report on their responses.

App Name	VIN	Location	Phone	Email
HondaLink	**Amplitude**	**Amplitude**		
Lincoln	ContentSquare			
MyNISSAN	**Alchemer**			**Alchemer**
myCadillac	**Adobe**, Acxiom **ContentSquare**, FullStory, Google, Meta, Microsoft, Pinterest, Snap, Yahoo	**ContentSquare**		**Adobe**, **ContentSquare**
myChevrolet	**Adobe**, Acxiom ContentSquare, FullStory, Google, Meta, Microsoft, Pinterest, Snap, Yahoo	**Adobe**		**Adobe**
myBuick	**Adobe**, Acxiom **ContentSquare**, FullStory, Google, Meta, Microsoft, Pinterest, Snap, Yahoo			**Adobe**, **ContentSquare**
myGMC	**Adobe**, Acxiom **ContentSquare**, FullStory, Google, Meta, Microsoft, Pinterest, Snap, Yahoo	**ContentSquare**	**ContentSquare**	**Adobe**, **ContentSquare**

Table 6: Seven companion mobile apps shared PII with ATA third parties. Bolded companies received VIN and at least one other form of PII from the same app.

6.1 Compliance with Privacy Policies

We focus on the mobile apps we observed to be sharing PII, and manually reviewed the privacy policies of the seven apps listed in Table 6 in May 2025. We found that all manufacturers that shared PII were disclosing that they may share PII with third parties, but not which third parties or the purposes for data flows. GM (myChevrolet, myCadillac, myBuick, myGMC), Lincoln, and Nissan disclosed that they shared VINs with third parties. Nissan questionably asserted that sharing a vehicle's VIN was more privacy preserving than sharing other types of unique identifiers.

Honda's policy stated that—excepting IP addresses—user geolocation data was not sold or used for third party advertising. We note that Amplitude—with whom VIN and precise location data was shared by the HondaLink App—is a product analytics and event tracking platform, not an advertiser. In addition, Honda's policy considers VINs to be "commercial information" that may be used for marketing and advertising. After we disclosed our findings, Honda stated that, in response to our study, they requested that Amplitude delete all received location data and updated the HondaLink app to no longer send geolocation to Amplitude.

6.2 Disclosure Responses

In light of our privacy-relevant findings, we reached out to 17 of the 18 manufacturers represented in our study to disclose our findings and inquire about the reason for this activity.[9] Within the 14 responses, we noticed three main categories of explanations:

1. Reliance on third party service contracts: All responding manufacturers stated that the data flows we observed were in line with the contracts they have with their third party service providers,

[9]We did not contact Fisker, which went out of business before our outreach.

and that those contracts prohibit use of PII beyond what is outlined in their privacy policy. However, as previously investigated by Mozilla [19] and described in § 6.1, these policies and agreements are often overbroad and expansive. Additionally, even if the contracts are in place and are followed, each additional recipient of personal data increases the probability of a privacy breach [37].

2. "It's the *embedded browser* that the app relies on": Five manufacturers argued that their apps do not share data with third parties. Instead, they argued that some links in their apps open webpages within an embedded browser—without the user's knowledge or warning—and that there may be third parties on those embedded webpages that collect data. Three of these manufacturers also asserted that these embedded webpages would prompt the user to accept or reject any ATA cookies. However, in our review of the recordings of companion app interaction testing, we did not find this to always be the case.

3. Handling software-defined vehicles is the consumer's responsibility: Many of the vehicles in our sample include sophisticated infotainment systems that are powered by rich operating systems (e.g., from Google) and contain apps developed by third parties (e.g., Spotify). Seven manufacturers stated that it is the consumer's responsibility to read through and accept all individual third-party terms of service agreements associated with in-vehicle software, even if that software comes pre-installed with the vehicle. However, we believe that this burden of responsibility does not provide owners with agency. Assuming owners can find the particular agreements, if an owner decides they are uncomfortable with the data sharing described within them, they are faced with (arguably) unfair choices: accept the agreements regardless of their concerns, forego the use of a connected-vehicle feature, or stop using the vehicle entirely. For example, if an owner declines Tesla's data sharing agreement, the owner is faced with a stern warning [95]:

> *This may result in your vehicle suffering from reduced functionality, serious damage, or inoperability.*

Disabling Rivian's data collection agreement results in the following warning [83]:

> *It will limit or disable certain functionality in the vehicle (e.g., navigation, lane keeping assistance, and over-the-air updates, which provide new features, better performance, safety enhancements, and bug fixes).*

Key Takeaways

1. Existing privacy policies are overly broad and lack transparency regarding the storage, sharing, or selling of consumer data.
2. Many manufacturers do not provide the consumer with meaningful or easy ways to opt out of data collection and sharing.

7 Conclusion

This paper presented the first large-scale, exploratory analysis of the connected-vehicle ecosystem from the perspective of network communications from vehicles and their companion mobile apps. We developed a multi-phase and multi-modal testing methodology to provide new insight into network transmissions from 21 vehicles across Wi-Fi and cellular, and how this relates to the information exchanged over the Internet by 30 vehicle companion mobile apps.

We found that vehicles, under a variety of real-world settings, contact not only a wide range of first parties (i.e., manufacturer domains) and car-specific support parties, but also third parties that are known to provide advertising and tracking services. Interestingly, the connected vehicle ecosystem exhibits a high level of diversity—even vehicles from the same manufacturer exhibit different network behaviors. When adding vehicle companion apps to the analysis, we found that vehicle owners are exposed to even more privacy-sensitive ATA communication—in some cases more than two dozen additional trackers. Six of the apps we tested transmitted multiple types of PII (e.g., email or geolocation) along with the vehicle-specific VIN to ATA services (Table 6), representing a unique tracking threat to vehicle owners. We disclosed our findings to manufacturers, leading to a variety of responses, but with a prevailing theme of shifting the burden of responsibility for data to the end user. As one notable exception, Honda improved its data collection practices to prevent sending precise geolocation to third parties.

Overall, our study revealed a large gap between what vehicle manufacturers publicly disclosed and how the connected vehicle ecosystem actually shares data over the Internet, which has explicit privacy implications. Based on the opaque nature of vehicular systems, we argue that there is a need for better transparency to ensure increased visibility into the entire ecosystem to identify and address corresponding harms.

8 Acknowledgements

The authors would like to thank Consumer Reports for collaborating with us and allowing for the use of their vehicles in our research. In particular we thank Jennifer Stockburger, Michael Crossen, John Ibbotson, Jake Fisher, Justin Brookman, and Derek Kravitz for their help in organizing the collaboration, coordination of site visits, media and manufacturer outreach.

We would also like to thank our anonymous reviewers and our shepherd for their helpful feedback. Additionally, we thank Athicha Srivirote and Jeffrey Gleason for accompanying on experiments.

This work was funded in part by NSF grants SaTC-1955227, SaTC-2144914, and CNS-2247307. The views expressed in this publication are those of the authors and do not necessarily represent the views of the United States, the Department of Homeland Security, the United States Coast Guard, the National Science Foundation, or Consumer Reports.

References

[1] Abbas Acar, Hossein Fereidooni, Tigist Abera, Amit Kumar Sikder, Markus Miettinen, Hidayet Aksu, Mauro Conti, Ahmad-Reza Sadeghi, and Selcuk Uluagac. 2020. Peek-a-Boo: I see your smart home activities, even encrypted!. In *Proc. of ACM WiSec* (Virtual Event). 207–218. doi:10.1145/3395351.3399421

[2] Gunes Acar, Steven Englehardt, and Arvind Narayanan. 2020. No boundaries: data exfiltration by third parties embedded on web pages. *Proc. on PETS* 2020, 2 (2020), 220–238. doi:10.2478/popets-2020-0070

[3] Dilawer Ahmed, Anupam Das, and Fareed Zaffar. 2022. Analyzing the Feasibility and Generalizability of Fingerprinting Internet of Things Devices. *Proc. on PETS* 2022, 2 (2022), 578–600. doi:10.2478/popets-2022-0057

[4] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. 2015. Your

Location Has Been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging. (2015), 787–796. doi:10.1145/2702123.2702210
[5] Amarisoft. n.d.. Amarisoft Callbox Classic product details. amarisoft.com. https://www.amarisoft.com/test-and-measurement/device-testing/device-products/amari-callbox-classic.
[6] Android Open Source Project. 2026. What Is Android Automotive? https://source.android.com/docs/automotive/start/what_automotive. Accessed 2026-08-14.
[7] Noah Apthorpe, Danny Yuxing Huang, Dillon Reisman, Arvind Narayanan, and Nick Feamster. 2019. Keeping the Smart Home Private with Smart(er) IoT Traffic Shaping. *Proc. on PETS* 2019, 3 (2019), 128–148. doi:10.2478/popets-2019-0040
[8] Automotive Testing Technology International. 2025. The Future of Automotive Operating Systems: Proprietary vs Open-Source Solutions. https://www.adt.media/software-defined-vehicles/how-good-are-automotive-operating-systems/101316. Accessed 2026-08-14; features commentary from Martin Schleicher, Head of Software Strategy at Continental.
[9] Belk Ford. 2022. Technology Features in the 2022 Ford F-150 Lightning. https://www.belkford.net/blog/2022/december/12/technology-features-in-the-2022-ford-f-150-lightning.htm. Dealer blog post. Accessed 2026-04-09.
[10] Reuben Binns. 2022. Tracking on the Web, Mobile and the Internet of Things. *Foundations and Trends in Web Science* 8, 1–2 (2022), 1–113. doi:10.1561/1800000029
[11] Eduardo Blázquez, Sergio Pastrana, Álvaro Feal, Julien Gamba, Platon Kotzias, Narseo Vallina-Rodriguez, and Juan Tapiador. 2021. Trouble Over-The-Air: An Analysis of FOTA Apps in the Android Ecosystem. In *Proc. of IEEE Symposium on Security and Privacy* (Virtual Event). 1606–1622. doi:10.1109/SP40001.2021.00095
[12] Chiara Bodei, Gianpiero Costantino, Marco De Vincenzi, Ilaria Matteucci, and Anna Monreale. 2023. Data Collection in Automotive: A Deep Analysis of Carmakers' Mobile App Privacy Policies. In *IEEE International Conference on Intelligent Transportation Systems* (Bilbao, ES). 425–432. doi:10.1109/ITSC57777.2023.10422449
[13] Chiara Bodei, Gianpiero Costantino, Marco De Vincenzi, Ilaria Matteucci, and Anna Monreale. 2023. Vehicle Data Collection: A Privacy Policy Analysis and Comparison. In *International Conference on Information Systems Security and Privacy* (Lisbon, PT). 626–633. doi:10.5220/0011779500003405
[14] Robin Bolz and Reiner Kriesten. 2021. Automotive Vulnerability Disclosure: Stakeholders, Opportunities, Challenges. *Journal of Cybersecurity and Privacy* 1, 2 (2021), 274–288. doi:10.3390/jcp1020015
[15] Buick. 2023. Buick Introduces First-Ever Envista. https://media.buick.com/media/us/en/buick/news.detail.html/content/Pages/news/us/en/2023/apr/0417-envista.html. Accessed 2026-04-28.
[16] Buick. 2024. Stay Connected with Google Built-In. https://www.buick.com/explore/news/google-built-in. Accessed 2026-04-28.
[17] Bureau of Industry and Security Office of Congressional and Public Affairs. 2025. Commerce Finalizes Rule to Secure Connected Vehicle Supply Chains from Foreign Adversary Threats. Department of Commerce. https://www.bis.gov/press-release/commerce-finalizes-rule-secure-connected-vehicle-supply-chains-foreign-adversary-threats.
[18] Cadillac. 2024. Google Built-In Apps. https://www.cadillac.com/technology/google-built-in. Official Cadillac product page listing 2024 LYRIQ as standard Google built-in vehicle.
[19] Jen Caltrider, Misha Rykov, and Zoe MacDonald. 2023. It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy. foundation.mozilla.org. https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy.
[20] Cars.com Staff. 2023. Finally, There's a New Lexus Multimedia System: 6 Things We Like, 2 We Don't. https://www.cars.com/articles/finally-theres-a-new-lexus-multimedia-system-6-things-we-like-2-we-dont-436892/. Accessed 2026-04-09.
[21] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. 2011. Comprehensive Experimental Analyses of Automotive Attack Surfaces. In *Proc. of USENIX Security Symposium* (San Francisco, USA).
[22] Aldo Cortesi, Maximilian Hils, and Thomas Kriechbaumer. 2025. mitmproxy - an interactive HTTPS proxy. mitmproxy.org.
[23] Bennett Cyphers and Gennie Gebhart. 2022. How to Disable Ad ID Tracking on iOS and Android, and Why You Should Do It Now. https://www.eff.org/deeplinks/2022/05/how-disable-ad-id-tracking-ios-and-android-and-why-you-should-do-it-now.
[24] Edmunds Staff. 2023. 2023 Land Rover Range Rover Sport First Drive: A Divine Improvement. https://www.edmunds.com/car-news/2023-land-rover-range-rover-sport-first-drive-a-divine-improvement.html. Accessed 2026-04-09.
[25] Edmunds Staff. 2023. Driving the 2023 Mercedes-Benz EQS SUV: Family Hauler with Plenty of Wow. https://www.edmunds.com/car-news/driving-the-2023-mercedes-benz-eqs-suv-family-hauler-with-plenty-of-wow.html. Accessed 2026-04-09.
[26] William Enck, Peter Gilbert, Seungyeop Han, Vasant Tendulkar, Byung-Gon Chun, Landon P. Cox, Jaeyeon Jung, Patrick McDaniel, and Anmol N. Sheth. 2010. TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones. In *Proceedings of the 9th USENIX Symposium on Operating Systems Design and Implementation (OSDI)*. USENIX Association, 393–407. doi:10.1145/2619091
[27] Steven Englehardt, Jeffrey Han, and Arvind Narayanan. 2018. I never signed up for this! Privacy implications of email tracking. *Proc. on PETS* 2018, 1 (2018), 109–126. doi:10.1515/popets-2018-0006
[28] John Faulkner. 2024. Road Test: 2024 Fiat 500e. Clean Fleet Report. https://cleanfleetreport.com/road-test-2024-fiat-500e/. Accessed 2026-04-09.
[29] Kassem Fawaz, Kyu-Han Kim, and Kang G Shin. 2016. Protecting privacy of BLE device users. In *Proc. of USENIX Security Symposium* (Austin, TX). 1205–1221.
[30] FCA North America. 2021. Press Release No. 21506. https://media.fcanorthamerica.com/newsrelease.do?id=21506&mid=1. Accessed 2026-04-09.
[31] Álvaro Feal, Paolo Calciati, Narseo Vallina-Rodriguez, Carmela Troncoso, and Alessandra Gorla. 2020. Angel or Devil? A Privacy Study of Mobile Parental Control Apps. *Proc. on PETS* 2020, 2 (2020), 314–335. doi:10.2478/popets-2020-0029
[32] Federal Trade Commission of the United States. 2026. FTC Finalizes Order Settling Allegations that GM and OnStar Collected and Sold Geolocation Data Without Consumers' Informed Consent. https://www.ftc.gov/news-events/news/press-releases/2026/01/ftc-finalizes-order-settling-allegations-gm-onstar-collected-sold-geolocation-data-without-consumers. Press release. Accessed 2026-04-06.
[33] Lisa Aronson Fontes. 2024. Abusers Are Monitoring and Spying on Victims Through Their Cars. domesticshelters.org. https://www.domesticshelters.org/articles/identifying-abuse/abusers-are-monitoring-and-spying-on-victims-through-their-cars.
[34] Imane Fouad, Nataliia Bielova, Arnaud Legout, and Natasa Sarafijanovic-Djukic. 2020. Missed by Filter Lists: Detecting Unknown Third-Party Trackers with Invisible Pixels. *Proc. on PETS* 2020, 2 (2020), 499–518. doi:10.2478/popets-2020-0038
[35] Julien Gamba, Mohammed Rashed, Abbas Razaghpanah, Juan Tapiador, and Narseo Vallina-Rodriguez. 2020. An Analysis of Pre-installed Android Software. In *Proc. of IEEE Symposium on Security and Privacy* (Virtual Event). 1039–1055. doi:10.1109/SP40000.2020.00013
[36] Alexander Gamero-Garrido, Kicho Yu, Sumukh Vasisht Shankar, Sachin Kumar Singh, Sindhya Balasubramanian, Alexander Wilcox, and David Choffnes. 2025. Empirically Measuring Data Localization in the EU. *Proc. on PETS* 2025, 3 (2025), 436–450. doi:10.56553/popets-2025-0107
[37] Seyed Ramin Ghorashi, Tanveer Zia, Michael Bewong, and Yinhao Jiang. 2023. An Analytical Review of Industrial Privacy Frameworks and Regulations for Organisational Data Sharing. *Applied Sciences* 13, 23 (2023), 12727. doi:10.3390/app132312727
[38] Jonathan M. Gitlin. 2023. The 2024 Chevrolet Blazer First Drive: GM's EV Platform Goes Mainstream. https://arstechnica.com/cars/2023/12/the-2024-chevrolet-blazer-first-drive-gms-ev-platform-goes-mainstream/. Accessed 2026-04-28.
[39] Green Car Reports Staff. 2024. 2024 Honda Prologue EV Test Drive Review. https://www.greencarreports.com/news/1142379_2024-honda-prologue-ev-test-drive-review. Accessed 2026-04-09.
[40] Tianbo Gu, Zheng Fang, Allaukik Abhishek, and Prasant Mohapatra. 2020. IoTSpy: Uncovering Human Privacy Leakage in IoT Networks via Mining Wireless Context. In *Proc. of the IEEE Symposium on Personal, Indoor and Mobile Radio Communications* (Virtual Event). 1–7. doi:10.1109/PIMRC48278.2020.9217236
[41] Dalton Hahn, Arslan Munir, and Vahid Behzadan. 2021. Security and Privacy Issues in Intelligent Transportation Systems: Classification and Challenges. *IEEE Intelligent Transportation Systems Magazine* 13, 1 (2021), 181–196. doi:10.1109/MITS.2019.2898973
[42] Subir Halder, Amrita Ghosal, and Mauro Conti. 2020. Secure over-the-air software updates in connected vehicles: A survey. *Computer Networks* 178 (2020), 107343. doi:10.1016/j.comnet.2020.107343
[43] Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel. 2008. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. In *Proceedings of the 29th IEEE Symposium on Security and Privacy (S&P)*. IEEE, 129–142.
[44] Bengt Halvorson. 2024. Review, Postmortem: Fisker Ocean Was a Promising EV, May Be Frozen in Beta. https://www.greencarreports.com/news/1143959_fisker-ocean-ev-test-drive-review-postmortem. Accessed 2026-04-28.
[45] Andrew J. Hawkins. 2021. Ford and Google Are Teaming Up on a Six-Year Partnership. The Verge. https://www.theverge.com/2021/2/1/22260176/ford-google-android-infotainment-os-2023. Accessed 2026-04-09.
[46] Kashmir Hill. 2023. Car Trackers and GPS Abuse. The New York Times. https://www.nytimes.com/2023/12/31/technology/car-trackers-gps-abuse.html.
[47] Kashmir Hill. 2024. Automakers Are Sharing Consumers' Driving Behavior With Insurance Companies. nytimes.com. https://www.nytimes.com/2024/03/

11/technology/carmakers-driver-tracking-insurance.html.
[48] Kashmir Hill. 2024. Automakers Sold Driver Data for Pennies, Senators Say. The New York Times. https://www.nytimes.com/2024/07/26/technology/driver-data-sold-for-pennies.html.
[49] Kashmir Hill. 2024. How G.M. Tricked Millions of Drivers Into Being Spied On (Including Me). nytimes.com. https://www.nytimes.com/2024/04/23/technology/general-motors-spying-driver-data-consent.html.
[50] Kashmir Hill and Surya Mattu. 2024. Regulators Investigate Carmakers' Driver Tracking. The New York Times. https://www.nytimes.com/2024/04/30/technology/regulators-investigate-carmakers-driver-tracking.html
[51] Danny Yuxing Huang, Noah Apthorpe, Frank Li, Gunes Acar, and Nick Feamster. 2020. Iot inspector: Crowdsourcing labeled network traffic from smart home devices at scale. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 4, 2 (2020), 1–21. doi:10.1145/3397333
[52] IPinfo Inc. [n. d.]. IPinfo for Academic Research. ipinfo.io. https://ipinfo.io/use-cases/ip-data-for-academic-research.
[53] Seonghoon Jeong, Minsoo Ryu, Hyunjae Kang, and Huy Kang Kim. 2023. Infotainment System Matters: Understanding the Impact and Implications of In-Vehicle Infotainment System Hacking with Automotive Grade Linux. In *Proc. of ACM CODASPY* (Charlotte, NC, US). 201–212. doi:10.1145/3577923.3583650
[54] Konrad Kollnig, Reuben Binns, Pierre Dewitte, Max Van Kleek, Ge Wang, Daniel Omeiza, Helena Webb, and Nigel Shadbolt. 2021. A Fait Accompli? An Empirical Study into the Absence of Consent to Third-Party Tracking in Android Apps. In *Proc. of SOUPS* (Virtual Event). 181–196.
[55] Kirsten Korosec. 2021. Lucid Motors Reveals All the Tech Inside Its All-Electric Air Sedan. TechCrunch. https://techcrunch.com/2021/05/26/lucid-motors-reveals-all-the-tech-inside-its-all-electric-air-sedan/.
[56] Martin Kotuliak, Simon Erni, Patrick Leu, Marc Röschlin, and Srdjan Čapkun. 2022. LTrack: Stealthy Tracking of Mobile Phones in LTE. In *Proc. of USENIX Security Symposium* (Boston, US). 1291–1306. doi:10.3929/ETHZ-B-000517466
[57] Daniel B. Kramer, Matthew Baker, Benjamin Ransford, Andres Molina-Markham, Quinn Stewart, Kevin Fu, and Matthew R. Reynolds. 2012. Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance. *PLOS ONE* 7, 7 (2012), e40200. doi:10.1371/journal.pone.0040200
[58] Derek Kravitz. 2025. Your Car May Be Spying On You. Here's How to Get It to Stop. https://www.consumerreports.org/electronics/personal-information/how-to-stop-your-car-from-collecting-sharing-driving-data-a1233378612/
[59] Denis Foo Kune, John Koelndorfer, Nicholas Hopper, and Yongdae Kim. 2012. Location leaks on the GSM air interface. In *Proc. of NDSS* (San Diego, US).
[60] Van Huynh Le, Jerry den Hartog, and Nicola Zannone. 2018. Security and privacy for innovative automotive applications: A survey. *Computer Communications* 132 (2018), 17–41. doi:10.1016/j.comcom.2018.09.010
[61] Lexus of Portland. 2024. Lexus RX Technology. https://www.lexusofportland.com/lexus-rx-technology/. Dealer webpage. Accessed 2026-04-09.
[62] Matthew Luckie, Bradley Huffaker, Alexander Marder, Zachary Bischof, Marianne Fletcher, and KC Claffy. 2021. Learning to Extract Geographic Information from Internet Router Hostnames. In *Proc. of ACM CoNEXT* (Virtual Event). 440–453. doi:10.1145/3485983.3494869
[63] Sahar Mazloom, Mohammad Rezaeirad, Aaron Hunter, and Damon McCoy. 2016. A Security Analysis of an In-Vehicle Infotainment and App Platform. In *10th USENIX Workshop on Offensive Technologies (WOOT 16)*. USENIX Association, Austin, TX. https://www.usenix.org/conference/woot16/workshop-program/presentation/mazloom
[64] Mercedes-Benz. 2023. Press Release: Mercedes-Benz and Google Collaboration. https://mercedes-benz-media.co.uk/releases/1517. Accessed 2026-04-09.
[65] Abdul Moiz and Manar H Alalfi. 2020. An Approach for the Identification of Information Leakage in Automotive Infotainment systems. In *IEEE Working Conference on Source Code Analysis and Manipulation* (Virtual Event). 110–114. doi:10.1109/SCAM51674.2020.00017
[66] Sen Nie, Ling Liu, and Yuefeng Du. 2017. Free-fall: Hacking Tesla from wireless to CAN bus. *Briefing, Black Hat USA* 25, 1, 16.
[67] Nissan North America, Inc. 2023. *2023 Nissan ARIYA® Product Brochure*. Nissan North America, Inc. https://www.nissanusa.com/content/dam/Nissan/us/vehicle-brochures/2023/2023-nissan-ariya-brochure-en.pdf. Official vehicle brochure. Accessed 2026-04-28.
[68] Eva Papadogiannaki and Sotiris Ioannidis. 2021. A Survey on Encrypted Network Traffic Analysis Applications, Techniques, and Countermeasures. *Comput. Surveys* 54, 6, Article 123 (July 2021), 35 pages. doi:10.1145/3457904
[69] Bryson R Payne. 2019. Car Hacking: Accessing and Exploiting the CAN Bus Protocol. *Journal of Cybersecurity Education, Research and Practice* 2019, 1 (2019), 5. doi:10.62915/2472-2707.1045
[70] Mert D. Pesé and Kang G. Shin. 2019. Survey of Automotive Privacy Regulations and Privacy-Related Attacks. SAE Technical Paper.
[71] Pinckney Chrysler Dodge Jeep Ram. 2025. 2025 RAM 1500 Technology. https://www.pinckneychryslerdodgejeepram.com/2025-ram-1500-technology/. Dealer webpage. Accessed 2026-04-09.
[72] Amogh Pradeep, Álvaro Feal, Julien Gamba, Ashwin Rao, Martina Lindorfer, Narseo Vallina-Rodriguez, and David Choffnes. 2023. Not Your Average App: A Large-scale Privacy Analysis of Android Browsers. *Proc. on PETS* 2023, 1 (2023), 29–46. doi:10.56553/popets-2023-0003
[73] Amogh Pradeep, Johanna Gunawan, Alvaro Feal, Woodrow Hartzog, and David Choffnes. 2025. Gig Work at What Cost? Exploring Privacy Risks of Gig Work Platform Participation in the US. *Proc. on PETS* 2025, 1 (2025), 491–510. doi:10.56553/popets-2025-0027
[74] Mark Quinlan, Jun Zhao, and Andrew Simpson. 2019. Connected Vehicles: A Privacy Analysis. (2019), 35–44. doi:10.1007/978-3-030-24900-7_3
[75] Md Abdur Rahim, Md Arafatur Rahman, Md Mustafizur Rahman, A Taufiq Asyhari, Md Zakirul Alam Bhuiyan, and D Ramasamy. 2021. Evolution of IoT-enabled connectivity and applications in automotive industry: A review. *Vehicular Communications* 27 (2021), 100285. doi:10.1016/j.vehcom.2020.100285
[76] Abbas Razaghpanah, Rishab Nithyanand, Narseo Vallina-Rodriguez, Srikanth Sundaresan, Mark Allman, Christian Kreibich, and Phillipa Gill. 2018. Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem. In *Proc. of NDSS* (San Diego, US). doi:10.14722/ndss.2018.23353
[77] Jingjing Ren, Daniel J Dubois, David Choffnes, Anna Maria Mandalari, Roman Kolcun, and Hamed Haddadi. 2019. Information Exposure From Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach. In *Proc. of IMC* (Amsterdam, NL). 267–279. doi:10.1145/3355369.3355577
[78] Jingjing Ren, Martina Lindorfer, Daniel Dubois, Ashwin Rao, David Choffnes, and Narseo Vallina-Rodriguez. 2018. Bug Fixes, Improvements, ... and Privacy Leaks A Longitudinal Study of PII Leaks Across Android App Versions. In *Proc. of NDSS* (San Diego, US). doi:10.14722/ndss.2018.23143
[79] Jingjing Ren, Ashwin Rao, Martina Lindorfer, Arnaud Legout, and David Choffnes. 2016. ReCon: Revealing and Controlling PII Leaks in Mobile Network Traffic. In *Proc. of MobiSys* (Singapore, SG). 361–374. doi:10.1145/2906388.2906392
[80] ResearchAndMarkets.com. 2021. Global Consumer Automobile Entertainment Market 2021 to 2026: Manufacturer vs. Third-Party Connected Vehicle Infotainment Apps. https://www.businesswire.com/news/home/20210203005694/en/Global-Consumer-Automobile-Entertainment-Market-2021-to-2026---Manufacturer-vs.-Third-party-Connected-Vehicle-Infotainment-Apps---ResearchAndMarkets.com. Accessed 2026-08-14; press release announcing report addition to ResearchAndMarkets.com, distributed via Business Wire.
[81] Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, and Serge Egelman. 2018. "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. *Proc. on PETS* 2018, 3 (2018), 63–83. doi:10.1515/popets-2018-0021
[82] RIPE Network Coordination Center. [n. d.]. How RIPE Atlas works. ripe.net. https://www.ripe.net/analyse/internet-measurements/ripe-atlas/how-ripe-atlas-works.
[83] Rivian Automotive, Inc. 2025. Can I Disable All Data Collection From My Vehicle? https://rivian.com/support/article/can-i-disable-all-data-collection-from-my-vehicle. Accessed 2026-04-29.
[84] Said Jawad Saidi, Anna Maria Mandalari, Roman Kolcun, Hamed Haddadi, Daniel J. Dubois, David Choffnes, Georgios Smaragdakis, and Anja Feldmann. 2020. A Haystack Full of Needles: Scalable Detection of IoT Devices in the Wild. In *Proc. of IMC*. doi:10.1145/3419394.3423650
[85] Yeonghun Shin, Sungbum Kim, Wooyeon Jo, and Taeshik Shon. 2022. Digital forensic case studies for in-vehicle infotainment systems using Android Auto and Apple CarPlay. *Sensors* 22, 19 (2022), 7196. doi:10.3390/s22197196
[86] Clint Simone. 2023. Driven: The 2024 Ford Mustang EcoBoost Focuses on the Details. Edmunds. https://www.edmunds.com/car-news/driven-the-2024-ford-mustang-ecoboost-focuses-on-the-details.html. Accessed 2026-04-09.
[87] Arunan Sivanathan, Hassan Habibi Gharakheili, Franco Loi, Adam Radford, Chamith Wijenayake, Arun Vishwanath, and Vijay Sivaraman. 2019. Classifying IoT Devices in Smart Environments Using Network Traffic Characteristics. *IEEE Transactions on Mobile Computing* 18, 8 (2019), 1745–1759. doi:10.1109/TMC.2018.2866249
[88] Stellantis North America. 2024. Press Release: 2024 Fiat 500e. https://embargoed.stellantisnorthamerica.com/newsrelease.do?id=24067&mid=1469. Accessed 2026-04-09.
[89] Alanoud Subahi and George Theodorakopoulos. 2018. Ensuring Compliance of IoT Devices with Their Privacy Policy Agreement. In *IEEE International Conference on Future Internet of Things and Cloud* (Barcelona, ES). 100–107. doi:10.1109/FiCloud.2018.00022
[90] TechCrunch Staff. 2024. Rivian Refresh: R1T and R1S Second Generation – Speed, Range, Apple and Google. https://techcrunch.com/2024/06/06/rivian-refresh-r1t-r1s-second-generation-speed-range-apple/. Accessed 2026-04-09.
[91] TechRater. 2023. Jaguar Land Rover Pivi and Pivi Pro Infotainment System. https://www.techrater.co.uk/motoring/jaguar-land-rover-pivi-pivi-pro-infotainment-system/. Accessed 2026-04-09.
[92] Matthew A. Telfor, Bryson R. Payne, and Tamirat T. Abegaz. 2025. Reverse Engineering the CAN Bus: Vulnerability Analysis in the Tesla Model 3. In *Security and Management and Wireless Networks*. 478–489. doi:10.1007/978-3-

031-86637-1_35
[93] Tesla, Inc. 2018. Tesla Linux Source Code Repository. https://github.com/teslamotors/linux.
[94] Tesla, Inc. 2024. SIM Card - Car Computer (Remove and Replace). https://service.tesla.com/docs/Model3/ServiceManual/2024/en-us/GUID-AE8A30A2-3BB5-419F-B046-381D9F972E43.html.
[95] Tesla, Inc. 2025. Privacy Notice: Choice and Transparency. https://www.tesla.com/legal/privacy#choice-and-transparency. Accessed 2026-04-29.
[96] Toyota Motor Corporation. 2023. Subaru Software Updates. https://www.toyota.com/firmware-updates/subaru/us/en/home. Accessed 2026-04-28.
[97] Toyota Motor North America. 2023. Revealed: First-Ever 2023 Toyota Corolla Cross Hybrid. https://pressroom.toyota.com/revealed-first-ever-2023-toyota-corolla-cross-hybrid/. Press release. Accessed 2026-04-09.
[98] TrueCar. 2024. 2024 Cadillac LYRIQ Review: Pricing, Trims & Photos. https://www.truecar.com/overview/cadillac/lyriq/2024/. Accessed 2026-04-28.
[99] Hayley Tsukayama, Eva Galperin, and Catalina Sanchez. 2024. Modern Cars Can Be Tracking Nightmares. Abuse Survivors Need Real Solutions. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2024/07/modern-cars-can-be-tracking-nightmares-abuse-survivors-need-real-solutions.
[100] Nisha Vinayaga-Sureshkanth, Raveen Wijewickrama, Anindya Maiti, and Murtuza Jadliwala. 2022. An Investigative Study on the Privacy Implications of Mobile E-scooter Rental Apps. In *Proc. of ACM WiSec* (San Antonio, US). 125–139. doi:10.1145/3507657.3528551
[101] Volvo Cars Mission Viejo. 2024. 2024 Volvo C40 Overview. https://www.volvocarsmissionviejo.com/blog/2024-volvo-c40-overview. Dealer blog post. Accessed 2026-04-09.
[102] Jun Yeon Won, Wenzhuo Wang, Keith Redmill, and Zhiqiang Lin. 2025. CarPlay at Risk: Unveiling Security Threats of Third-Party Infotainment Adapters. In *3rd USENIX Symposium on Vehicle Security and Privacy (VehicleSec 25)*. USENIX Association, Seattle, WA, 143–159. https://www.usenix.org/conference/vehiclesec25/presentation/won
[103] Peifu Yang, Yuhong Nan, Lei Xue, Yuliang Zhang, Juan Zhai, and Zibin Zheng. 2024. Understanding Privacy Risks of Intelligent Connected Vehicles Through Their Companion Mobile Apps. *IEEE Internet of Things Journal* 11, 20 (2024). doi:10.1109/JIOT.2024.3432778
[104] Wei Zhang, Yan Meng, Yugeng Liu, Xiaokuan Zhang, Yinqian Zhang, and Haojin Zhu. 2018. HoMonit: Monitoring Smart Home Apps from Encrypted Traffic. In *Proc. of ACM SIGSAC* (Toronto, Canada). 1074–1088. doi:10.1145/3243734.3243820
[105] Kai Zhao and Lina Ge. 2013. A Survey on the Internet of Things Security. (2013), 663–667. doi:10.1109/CIS.2013.145
[106] Sebastian Zimmeck, Peter Story, Abhilasha Ravichander, Daniel Smullen, Ziqi Wang, Joel Reidenberg, N. Cameron Russell, and Norman Sadeh. 2019. MAPS: Scaling Privacy Compliance Analysis to a Million Apps. *Proc. on PETS* 2019, 3 (2019), 66–86. doi:10.2478/popets-2019-0037
[107] Sebastian Zimmeck, Ziqi Wang, Lieyong Zou, Roger Iyengar, Bin Liu, Florian Schaub, Shormir Wilson, Norman Sadeh, Steven M. Bellovin, and Joel Reidenberg. 2017. Automated Analysis of Privacy Requirements for Mobile Apps. In *Proc. of NDSS* (San Diego, US). doi:10.14722/ndss.2017.23034
[108] Ryan ZumMallen. 2021. 2023 Subaru Solterra: Is the Outdoorsy EV Ready for Its Close-Up? https://www.edmunds.com/car-news/is-the-outdoorsy-ev-ready-for-its-close-up.html. Accessed 2026-04-28.

A Ethics

In this study, we performed controlled experiments with vehicles owned by Consumer Reports. As we note in § 3.2.1, all experiments were performed on premises at Consumer Reports: our experiments did not impact people outside of our research team, vehicles owned by other people, or public roadways. Our study does not qualify as human subjects research nor require IRB review.

As we discuss in § 3.2.2, we complied with FCC regulations when we were performing cellular experiments. Our experiments had no impact on public cellular networks as we conducted all cellular blocking and private cellular network advertising within the confines of a professionally-produced Faraday tent.

We observed vehicles and companion apps engaging in behaviors that are troubling from a privacy perspective. We responsibly disclosed these issues to manufacturers, provided ample time for response, and include a summary of their reasoning and responses in Section 6.2.

B Appendix

Source	App / Vehicle	Country	SLD	3P
Wi-Fi	Fiat 500e	Netherlands	tomtom.com	✓
	Ford F150 Lightning	Netherlands	trafficmanager.net	✓
	Lucid Air Touring	Ireland	facebook.com	✓
	Lucid Air Touring	Ireland	here.com	✓
	Tesla Cybertruck	Ireland	microsoft.com	✓
	Volvo C40	Ireland	volvo.care	
	Volvo C40	Netherlands	volvo.care	
App	Chrysler	Germany	xtn-lab.it	✓
	Maserati Connect	Ireland	fcagcv.com	
	MINI	Germany	bmwgroup.com	
	My BMW	Germany	bmwgroup.com	
	My BMW	Germany	dynatrace.com	✓
	MyHyundai	Canada	streamtheworld.com	✓
	MyHyundai	Netherlands	loopme.me	✓
	Volvo Cars	Ireland	volvo.care	
	Volvo Cars	Ireland	volvocars.com	

Table A1: Five vehicles and six companion mobile apps in our sample contacted a total of 13 IP addresses outside the US.

App Name	Ignored Hosts
Chrysler	["appdig-myconnect.chrysler.com", ".sdpr-02.fcagcv.com"]
Fiat	["appdig-myconnect.fiat.com", ".sdpr-02.fcagcv.com"]
FordPass	[]
GenesisIA	["api.telematics.genesismotorsusa.com", "revgeocode.search.hereapi.com"]
HondaLink	[".*honda.*"]
Jeep	["appdig-myconnect.jeep.com", ".sdpr-02.fcagcv.com"]
KiaAccess	['api.owners.kia.com']
Land Rover Remote	["haine.approoval.com", "mr.fullstory.com"]
Lexus	['.*lexus.*']
Lucid Motors	[]
Maserati Connect North America	["appdig-myconnect.maserati.com", ".sdpr-02.fcagcv.com"]
Mercedes-Benz (USA/CA)	[]
MINI	['.*bmw.*']
My BMW	['.*bmw.*']
myBuick	['.*gm.*']
myCadillac	['.*gm.*']
myChevrolet	['.*gm.*']
myGMC	['.*gm.*']
MyHyundai with Bluelink	['api.telematics.hyundaiusa.com']
MyMazda	[]
MyNISSAN	['.*nissancloud.*', '.*nissanusa.*']
MySubaru	[]
myVW	[".*vw.*"]
RAM	["appdig-myconnect.ramtrucks.com", ".sdpr-02.fcagcv.com"]
Rivian	[]
Subaru Solterra Connect	["subarudriverslogin.com", ".telematicsct.com"]
Tesla	[]
Lincoln	[]
Toyota	['.*toyotadriverslogin.*', '.*telematicsct.*']
Volvo Cars	[]

Table A2: Regex patterns that we gave to `mitmproxy` to ignore particular hosts. This was necessary because some apps had pinned certificates for a subset of domains.

	Unique SLDs			
Vehicle	**ATA**	**Integrated**	**Support**	**1st Party**
Tesla Model 3	34	36	7	2
Tesla Cybertruck	23	37	4	2
Cadillac Lyriq	10	21	2	2
Lucid Air	9	15	2	4
Chevrolet Blazer	7	18	2	2
Honda Prologue	5	18	2	1
Volvo C40	3	6	1	2
Rivian R1S	2	10	6	2
Ford F150	1	6	12	2
Ford Mustang	1	2	3	1
Toyota Corolla Cross	1	1	0	1
RAM 1500 Bighorn	0	5	0	1
Fiat 500e	0	5	0	1
Dodge Hornet	0	5	0	1
Subaru Solterra	0	4	0	2
Lexus NX450h	0	3	1	1
Fisker Ocean	0	2	1	1
Nissan Ariya	0	1	1	1
Land Rover Range Rover	0	0	1	1
Mercedes EQS	0	0	0	1
Buick Envista	0	0	0	1

Table A3: Vehicles sorted by the count of unique ATA SLDs they contacted via Wi-Fi. We present ATA associated, integrated, support, and first party SLDs contacted per vehicle.

	Unique SLDs		
App Name	**ATA**	**Integrated**	**Support**
myCadillac	51	12	5
myBuick	47	11	3
My BMW	47	7	6
Toyota	47	4	6
myGMC	45	11	5
myChevrolet	43	8	5
MyMazda	40	9	8
MyNISSAN	39	11	4
Lucid	26	4	2
MINI	22	10	3
FordPass	19	8	8
Rivian	16	6	4
Fiat	14	3	1
Lincoln	13	7	9
KiaAccess	11	10	1
Tesla	9	4	1
Maserati Connect	7	4	1
RAM	6	5	1
HondaLink	6	6	6
Lexus	6	2	0
Volvo	6	5	4
myVW	4	3	1
MySubaru	4	1	1
Jeep	3	4	1
Chrysler	3	4	1
Land Rover	3	3	0
Subaru Solterra Connect	3	2	1
MercedesBenz	2	3	1
MyHyundai	2	3	0
GenesisIA	0	1	0

Table A4: Companion apps that we studied, sorted by the count of unique ATA SLDs they contacted. We present ATA associated, integrated, and support SLDs contacted per vehicle.

		Unique SLDs		
Company Name	**Vehicles**	**ATA**	**Integrated**	**Support**
Alphabet Inc	13	11	12	1
Amazon	12	3	7	5
Spotify	8	3	4	0
Liberty Media Corporation	7	0	1	0
Cloudflare, Inc	6	0	1	2
Microsoft	6	2	2	5
TomTom International B.V.	5	0	1	0
HERE Global B.V.	4	0	2	0
Mapbox	4	0	1	0
Meta Platforms, Inc.	3	2	0	0
Fox Corporation	3	0	1	0
Metair Investments Limited	3	0	1	0
Thomson Reuters Corp	3	0	1	0
Connected Tech Io.	3	0	1	0
TuneIn Inc.	3	0	1	0
Miteno Communication Technology	3	1	0	0
iHeartMedia, Inc.,	3	0	2	0
Comscore, Inc	3	1	0	0
Comcast	3	0	1	0
Deutsche Welle	3	0	1	0
Podtrac	2	1	0	0
Branch Metrics Inc.	2	1	0	0
The Trade Desk	2	1	0	0
Telenav	2	0	1	0
Mixpanel	2	1	0	0
National Public Radio	2	0	1	0
Network Time Foundation	2	0	0	1
OneTrust	2	2	0	0
Endeavor Business Media	2	1	0	0
ByteDance Ltd.	2	2	11	0
ChargePoint Holdings, Inc.	2	0	1	0
Samsung Electronics	2	0	1	0
Sentry (Analytics)	2	1	0	0
Braze	2	2	0	0
Thales Group	2	0	0	1
Libsyn	2	0	1	0
INRIX, Inc.	2	1	0	0
Zoom	2	0	1	0
Amplitude Inc.	2	1	0	0
Unknown Parent Company	2	0	1	2
Snap Inc.	2	2	0	0
Akamai Technologies	2	0	0	2
TuneIn Inc.	2	0	1	0
Intel Corporation	2	0	0	1
U.S. Department of Commerce	1	0	0	1
X	1	3	0	0
Zeta Global	1	1	0	0
SoundHound AI	1	0	1	0
SquareUp	1	0	1	0
Yahoo	1	2	0	0
Stingray	1	0	2	0
Tealium	1	2	0	0
SurferNETWORK	1	0	1	0
VideoAmp	1	1	0	0
UNPKG	1	0	0	1
System76, Inc.	1	0	0	1
EVgo Inc.	1	0	1	0
Rokt	1	1	0	0
Episerver	1	1	0	0
Dr Teri Fisher	1	0	1	0
Freedom Holding Corp	1	0	1	0
Garmin Ltd.	1	0	1	0
General Infrastructure	1	0	0	1
Disney	1	1	1	0
Hulu	1	0	1	0
IBM	1	0	0	1
Impact Tech, Inc.	1	1	0	0
Jivox	1	1	0	0
DataDog	1	1	0	0
LiveXLive	1	0	1	0
DISH Network	1	0	1	0
Mediaocean	1	1	0	0
Cloudflare, Inc.	1	0	0	1
Adobe	1	2	0	0
MobileFuse, LLC	1	1	0	0
Netflix	1	0	4	0
Nextdoor Holdings, Inc.	1	1	0	0
Nielsen Holdings plc	1	2	0	0
PowerDNS.com B.V.	1	0	0	1
Acast	1	0	1	0

Table A5: Third-party companies contacted by vehicles in our sample over Wi-Fi, sorted by count of unique vehicles. We also present the total and unique number of domains associated with each company.

Company Name	Apps	Unique SLDs		
		ATA	Integrated	Support
Alphabet Inc	28	179	192	8
Adobe	15	106	0	0
Meta Platforms, Inc.	15	28	0	0
Microsoft	12	56	10	19
OneTrust	12	29	0	0
Akamai Technologies	11	0	0	72
Pinterest	9	17	0	0
Reddit	9	27	0	0
Amazon	7	13	0	15
Apollo	7	8	0	0
ContentSquare	7	57	0	0
Experian	7	9	0	0
FullStory (Google Invested)	7	14	0	0
Here Technologies	7	0	27	0
Neustar	7	9	0	0
Silver Lake	7	0	13	0
Snap Inc.	7	21	0	0
Catamorphic Co.,	6	0	17	0
DataDog	6	6	0	0
Dynatrace, LLC	6	10	0	0
Mapbox	6	0	17	0
The Trade Desk	6	17	0	0
Yahoo	6	6	0	0
Branch Metrics Inc.	5	9	0	0
Cisco Systems, Inc.	5	7	0	0
Emplifi	5	19	0	0
Medallia	5	18	0	0
SAP	5	7	0	0
iSpot.tv	5	5	0	0
Acxiom LLC	4	4	0	0
Barclays PLC	4	0	0	0
ByteDance Ltd.	4	6	0	0
Conversant	4	7	0	0
DocuSign, Inc.	4	0	4	0
Elettronica S.p.A.	4	0	4	0
General Motors	4	0	0	0
OpenJS Foundation	4	0	0	4
Stellantis	4	0	0	0
Unknown Parent Company	4	9	4	0
Alchemer (aka Alchemer Mobile)	3	3	0	0
American Automobile Association (AAA)	3	0	12	0
Approov	3	0	6	0
AtData	3	4	0	0
Brightcove	3	6	0	4
Cloudflare, Inc.	3	0	0	4
Intuition Machines, Inc.	3	0	7	0
Nordic Capital	3	6	0	0
Offspring Capital	3	3	0	0
Tealium	3	3	0	0
Amplitude Inc.	2	2	0	0
Coveo	2	2	0	0
CrazyEgg	2	8	0	0
Crownpeak	2	2	0	0
Ford Motor Company	2	0	0	0
Francisco Partners and TPG Inc.	2	4	0	0
Freepik Company S.L.U.	2	0	0	2
Mediaocean	2	5	0	0
Open-source project at github.com/unpkg	2	0	0	2
OpenX Software Ltd.,	2	2	0	0
Salesforce, Inc.	2	5	5	0
Spotify Technology S.A.	2	2	2	0
V99, Inc.	2	0	2	0
Vimeo.com, Inc.	2	10	0	0
X Corp.	2	2	0	0
open-source project at github.com/rdegges/ipify-api	2	0	0	2
open-source project part of CDN Alliance	2	0	0	2
Adobe Inc.	1	1	0	0
American List Counsel	1	1	0	0
AppsFlyer	1	10	0	0
AudioEye	1	2	0	0
AutoIntel, Inc.	1	1	0	0
BMW Group	1	0	0	0
Bread Financial	1	1	0	0
Brookfield Business Partners	1	1	0	0
CJK Group, Inc.	1	0	1	0
Cars Commerce, Inc	1	1	0	0
ChargePoint Holdings, Inc.	1	0	1	0
Cint Group	1	1	0	0
Contentful	1	2	0	0
Cox Enterprises, Inc.	1	0	3	0
Criteo	1	1	0	0
Datadog, Inc.	1	1	0	0
DevvStream Inc.	1	0	0	1
Dun & Bradstreet	1	1	0	0
EVgo Services, LLC	1	0	1	0
Elastic N.V.	1	0	0	1
Episerver	1	4	0	0
Fastly, Inc.	1	0	0	1
Geely Holding Group	1	0	0	0
Global Media & Entertainment Ltd	1	1	0	0
Honda Motor Co.	1	0	0	0
Impact Tech, Inc.	1	0	0	1
InMarket Media, LLC	1	3	0	0
InMobi	1	1	0	0
Index Exchange	1	1	0	0
Kantar Group	1	1	0	0
Ketch Kloud, Inc	1	0	0	2
Kia Corporation	1	0	0	0
Liberty Media Corporation	1	2	1	0
Liberty Mutual Insurance Company	1	0	4	0
LivePerson, Inc.	1	0	3	0
LiveRamp Holdings, Inc.	1	1	0	0
Lucid Group, Inc.	1	0	0	0
MSD Telematics Pvt Ltd	1	1	0	0
Magnite Inc.	1	2	0	0
Mazda Motor Corporation	1	0	0	0
Mercedes-Benz Group AG	1	0	0	0
Miteno Communication Technology	1	3	0	0
Mixpanel	1	1	0	0
New Country Motor Car Group. Inc.	1	0	0	0
Nextgen Technology Ltd.	1	0	1	0
Nexxen International Ltd	1	1	0	0
Nissan Motor Co.	1	0	0	0
OpenWeather Ltd	1	0	2	0
Outbrain	1	3	0	0
Press Ganey Forsta	1	0	1	0
PubMatic, Inc.	1	1	0	0
Qualia	1	1	0	0
Quantum Metric	1	2	0	0
Quiq, Inc.	1	0	1	1
Rengage	1	1	0	0
Rivian Automotive, Inc.	1	0	0	0
Roper Technologies	1	2	0	0
Sanctus LLC	1	1	0	0
Sentry	1	2	0	1
Sierra Technologies, Inc.	1	0	1	0
Smart Digital GmbH	1	1	0	0
SpeedCurve	1	2	0	0
StackAdapt	1	1	0	0
Station Digital Media	1	1	0	0
Statsig	1	2	0	0
Subaru Corporation	1	0	0	0
T-Mobile	1	1	0	0
Tesla, Inc.	1	0	0	0
Thoma Bravo, LP	1	0	1	0
TomTom N.V.	1	0	5	0
Toyota Group	1	0	0	0
Urgent.ly	1	0	1	0
Usercentrics	1	4	0	0
Verint	1	1	0	0
Volvo Car USA LLC	1	0	1	0
Zeta Global Holdings Corp.	1	10	0	0
accessiBe Inc.	1	0	3	0

Table A6: Third-party companies contacted by companion apps, sorted by count of unique vehicles. We also present the total and unique number of domains associated with each company.