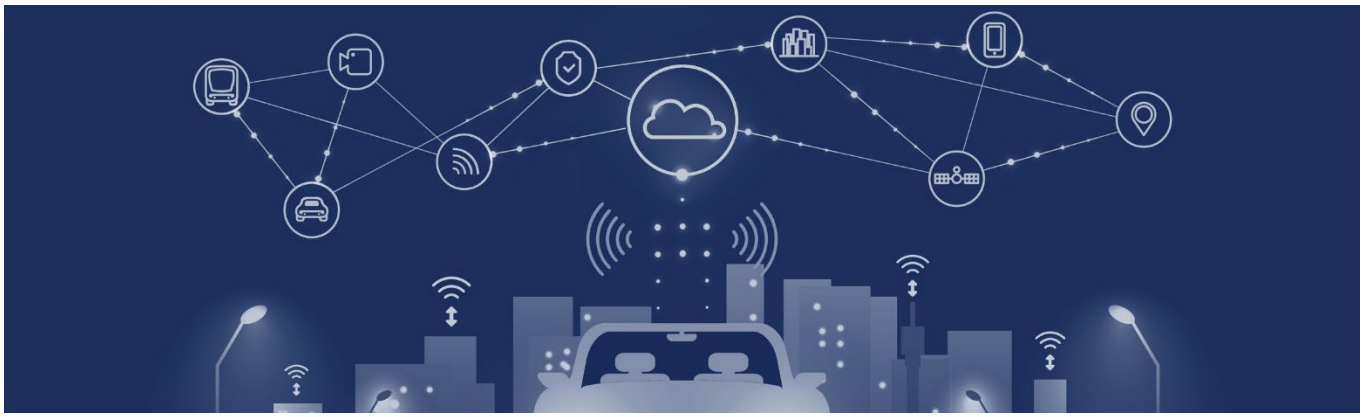
Cybersecurity and the Connected Car

James X. Dempsey and Andrew J. Grotto



June, 2024

AMERICAN CAR RENTAL ASSOCIATION

Executive Summary

The modern automobile is increasingly a mobile datacenter, generating large volumes of information and connected to the outside world. Traditionally, vehicle owners have owned the data about their cars. However, automobile manufacturers (OEMs) have begun to argue that they should assume the role of gatekeeper for this data. However, OEM gatekeeping is an outdated approach to cybersecurity, especially in a context where fleet managers have important, even safety-critical interests in data about the vehicles they own.

The data generated by cars can be used to advance important public policy goals. The incorporation of on-board computers into vehicle architecture has already yielded environmental benefits by optimizing engine performance and reducing emissions; safety improvements; and enhancements to the occupants' experience. Further benefits can be achieved through innovative use of data, especially with the ongoing transition to electric and automated vehicles.

Cybersecurity threats to automobiles are real. Demonstrated attacks have exploited widely-recognized security shortcomings in the data architecture adopted by the OEMs.

Fleet managers have compelling interests in unfiltered access to data from the cars they own, since they are responsible for car maintenance and have responsibilities for driver safety.

The gatekeeper model preferred by the OEMs is fundamentally inefficient. Moreover, it has no guarantee of serving the security interests that the OEMs cite as the justification for their approach. Indeed, the centralization of data poses its own risks to security and privacy. Instead, a decentralized model of data governance needs to be developed, which can simultaneously serve the needs of innovation *and* security.

The airline industry has not pursued a gatekeeper model for data generated by airplanes, despite having safety and cybersecurity concerns at least as serious as those of the automobile industry. Instead, it has developed a complex ecosystem based on multi-directional data flows, based on the principle that the airlines (the fleet managers) control the data about their planes.

Automobile OEMs have a poor record on cybersecurity and privacy. Their outmoded data architecture, characterized by high volumes of software code, complexity, and supply chain risk, poses serious cybersecurity risks.

OEMs and fleet managers need to commit to a set of data governance practices suited to a decentralized connected car ecosystem. These include adopting a risk-based and threat-informed approach to security design, agreeing on clear practices around driver and/or occupant consent and secondary uses of data, applying the principle of defense in depth to security policies and controls, implementing data encryption and attack-resistant methods of authentication, and undertaking continuous monitoring, testing, and improvement of the security architecture.

Cybersecurity and the Connected Car

James X. Dempsey and Andrew J. Grotto

Introduction

The modern automobile is increasingly a mobile datacenter, outfitted with dozens of sensors and electronic control units generating very large volumes of information and connected to the outside world. Traditionally, vehicle owners have owned the data about their cars. However, automobile manufacturers (OEMs) have begun to argue that they should assume the role of gatekeeper and control the flow of data to and from vehicles. We address here the cybersecurity arguments for and against the OEM gatekeeper model.

We begin by providing a general overview of the networks, processors, and sensors in current and anticipated future generations of automobiles. We then summarize the growing research literature on the cybersecurity risks of automobiles. We next explain why the gatekeeper model is a largely discredited approach to security, especially for an ecosystem like the one represented by the connected car, where multiple parties have legitimate interests in the data. We note that the aviation sector, with equally serious concerns about safety and cybersecurity, has a much more decentralized and collaborative approach to data access.

Our analysis of the gatekeeper model acknowledges that cybersecurity threats facing automobiles are real and pressing. However, we conclude that these risks are best addressed in a wider data governance context that examines alternative models for security, the incentives of OEMs and fleet owners to ensure that cyber risks are appropriately managed, and the risks to competition and innovation that the gatekeeper model presents. In our view, the security argument for OEMs serving as gatekeepers is weak, while the countervailing security and economic reasons for rejecting that role are strong.[1]

We were retained by the American Car Rental Association to provide this independent assessment of the cybersecurity issues associated with data flows to and from the cars of today and the near future. The views presented in this report are the authors' alone; we do not purport to speak on behalf of the American Car Rental Association or any other entity.

Overview of Cars as Mobile Datacenters

The modern automobile is a mobile datacenter, with (i) sensors gathering data from the vehicle, its occupants, and the outside world; (ii) processors extracting useful information from it; (iii) the vehicle and its occupants acting on that information; and (iv) cellular and other communications channels able to transmit data outside the car and to receive over-the -air (OTA) updates. Digital systems have replaced or augmented many of the mechanical components in cars, including acceleration, braking, and steering.

[1] There are also strong arguments, which we do not address here, that fleet owners need direct access to the vehicle's data in order to fulfill the owners' legal obligations regarding cybersecurity and privacy.

The incorporation of on-board computers into vehicle architecture has yielded environmental benefits by optimizing engine performance and reducing emissions; safety improvements such as airbags, antilock braking, electronic stability control, and rearview cameras; and improvements to the occupants' experience with enhanced infotainment options. And these benefits represent just the beginning of what can be achieved through innovative use of data, especially with the ongoing transition to electric and automated vehicles.

The current generation of non-automated cars typically has 70-100 electronic control units (ECUs)[2] controlling one or more electrical systems or subsystems in a vehicle, based on inputs from dozens or even hundreds of sensors monitoring vehicular functions ranging from engine performance to braking to door locks.[3] ECUs are linked together in one or more vehicular networks, with the most prevalent architecture being the controller area network (CAN). A vehicle's CAN networks carry its operational signals, such as acceleration and braking data, and broadcasts them across the CAN. A Local Interconnect Network (LIN) might handle non-operational functions, such as the instrument cluster, windows, seats, mirrors, rain and light sensors, and door locks, and interfaces with the CAN via an ECU. (Other car network protocols include Flexray and MOST.) Cameras support lane assist and rear view functionalities. Laser and radar technologies may also be present. Overall, the software running a car's systems is highly complex, typically featuring 100 million lines of computer code or more.

The in-vehicle infotainment (IVI) module, or headunit, often serves as a hub of information and in-vehicle functionality for the driver and passengers. Modern IVIs feature a touchscreen interface and can host a variety of apps, such as mapping, music, and vehicle performance. Headunits interface with the CAN to pull performance-related data in order to present visualizations of it to the vehicle occupants. For some vehicles, aftermarket headunits are available to replace the factory headunit.

Non-automated cars can generate 1-2 terabytes of raw data per day.[4] Automated vehicles will have additional sensors, such as LiDAR, and will produce far more data, on the order of 4 terabytes of data per hour.[5] As cars become more automated and electrified, their software will become more complex although the number of ECUs will fall as vehicle functions are consolidated.

For many years, the primary means of extracting data from a vehicle was through an on-board diagnostics (OBD) port. In the U.S., all cars are required by law to have an OBD-II port capable of interfacing with a vehicle's CAN networks. The original rationale for the requirement, which originated in California, was to facilitate emissions inspections, but the port has found use beyond emissions. For example, fleet operators use it to monitor and manage their fleets, including to manage services that improve the driver experience. Insurance companies use it to facilitate "pay as you drive" insurance plans. The OBD-II port has also turned out to be an important mechanism for repair shops, especially independent (non-OEM owned and operated) shops, to diagnose and fix problems.

Increasingly, automobiles are able to send and receive a variety of signals over the air. In many cars currently, there is a cellular connection (separate from the driver's smart phone) and a GPS device. In addition, headunits can typically be linked via bluetooth, USB connection, or WiFi to a smart device.

---

[2] Doug Burcicki, "The E/E architecture and the future of automotive innovation," *Siemans* (June 9, 2020), available at https://blogs.sw.siemens.com/ee-systems/2020/06/09/the-ee-architecture-and-the-future-of-automotive-innovation/.
[3] "Unlocking the Secrets: How Many Sensors Does Your Car Have," *DRex* (May 15, 2023), available at https://www.icdrex.com/unlocking-the-secrets-how-many-sensors-does-your-car-have/.
[4] Michele Bertoncello et al, "Unlocking the Full Life-Cycle Value From Connected Car Data," *McKinsey & Company* (February 11, 2021), available at https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/unlocking-the-full-life-cycle-value-from-connected-car-data.
[5] "Autonomous Cars Will Collect Approximately 4 TB of Data Every Hour of Driving," *Medium* (July 10, 2019), available at https://medium.com/@autodriveai/autonomous-cars-will-collect-approximately-4-tb- of-data-every-hour-of-driving-3819aba33204.

The next step may be V2X ("vehicle to everything communication") where cars communicate with other vehicles (V2V), with infrastructure (V2I), with pedestrians (V2P), and with other networks (V2N). Exchanged messages may be processed in edge computing servers, to support a variety of cooperative, connected, and automated mobility services, such as driver assistance, collision warning, and automatic emergency braking.[6] Such V2X technology has the potential to unlock completely new capabilities, functions, and solutions for drivers, pedestrians, responders, and everyone else who shares the road.[7]

Already, and increasingly, performance enhancements and safety recalls are accomplished with software updates delivered over the air. Tesla, for example, offers a variety of upgrades for a fee through over-the-air software updates.[8] General Motors offers over-the-air software update to many of its cars and trucks.[9] (Sometimes, these updates can cause problems: in November, Rivian pushed the wrong update and inadvertently disabled instrument panels and infotainment systems.[10])

Cybersecurity Risks to Cars

Cybersecurity threats to automobiles are real: researchers have been hacking cars for over a decade.[11] Early efforts involved physical access to the vehicle in order to exploit the OBD-II port. More recent research has focused on remote access via cellular, WiFi, bluetooth, and other radio connections. Many of the attacks demonstrated by this research involve exploiting widely recognized security shortcomings in the CAN protocol. These shortcomings include broadcasting all traffic to all network nodes; a priority-based packet arbitration scheme that is vulnerable to denial of service attacks; a lack of authenticator fields in CAN packets; lack of encryption; and weak access control.[12]

Two seminal articles in the catalog of automobile cybersecurity stand out. In "Experimental Security Analysis of a Modern Automobile" (2010), Koscher and co-authors demonstrated a range of attacks against "two late-model passenger cars (same make and model)" using physical access to the OBD-II port.[13] They developed a software tool called CARSHARK capable of analyzing CAN traffic and injecting packets, which they used to take adversarial control of critical operation functions, including engine performance and braking.

Although researchers in that first paper used direct physical access to the OBD-II port, a follow-on study by substantially the same research team, "Comprehensive Experimental Analyses of Automotive Attack Surface" (2011), demonstrated attacks on a "moderately priced late model sedan" using *remote* access vectors.[14] The authors identify three vectors: indirect physical access (e.g., via a smart device connected to the IVI), short-range wireless access, and long-range wireless access. For each

---

[6] Marco Centenaro et al, "Safety-Related Cooperative, Connected, and Automated Mobility Services," *IEEE Vehicular Technology Magazine* (Dec. 2021), available at https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9486856&tag=1.
[7] "V2X Explainer: The Basics on Vehicle-to-Everything Technology" (Aug. 9, 2023, updated March 27, 2024), available at https://www.haasalert.com/news/v2x-explainer.
[8] See Tesla, Upgrades webpage, https://www.tesla.com/support/upgrades.
[9] GM Service Bulletin, "Over the Air (OTA) and In Market Enhancement (IME) FAQs" (July 2023), available at https://static.nhtsa.gov/odi/tsbs/2023/MC-10239645-0001.pdf. See also Onstar, Vehicle software updates, https://www.onstar.com/support/faq/software-update-faq.
[10] Rivian, "2023.42 OTA Update Issue" (Nov. 2023), available at https://www.reddit.com/r/Rivian/comments/17usikn/202342_ota_update_issue/?rdt=49613
[11] Vipin Kumar Kukkala et al, "Roadmap for Cybersecurity in Autonomous Vehicles," *IEEE Consumer Electronics Magazine* (Jan. 19, 2022), available at https://arxiv.org/abs/2201.10349 and https://ieeexplore.ieee.org/document/9721088.
[12] The literature on CAN weaknesses is huge. See, for example, Damilola Oladimeji et al, "CANAttack: Assessing Vulnerabilities within Controller Area Network," *Sensors* (2023,) available at https://www.mdpi.com/1424-8220/23/19/8223; Robert Buttigieg et al, "Security Issues in Controller Area Networks in Automobiles" (2017), available at https://arxiv.org/pdf/1711.05824.pdf.
[13] Karl Koscher et al, "Experimental Security Analysis of a Modern Automobile," *2010 IEEE Symposium on Security and Privacy*, available at http://www.autosec.org/pubs/cars-oakland2010.pdf.
[14] Stephen Checkoway et al, "Comprehensive Experimental Analyses of Automotive Attack Surface" (2011), available at https://www.usenix.org/legacy/events/sec11/tech/full_papers/Checkoway.pdf.

of the three vectors, the authors demonstrated attacks capable of compromising the safety and performance of the targeted vehicle.

Among the most notorious of vehicle hacks is the one carried out by Miller and Valasec against a 2015 Jeep Cherokee. The car's OEM-installed headunit, Uconnect, was vulnerable to a remote attack, carried out over its cellular connection, that allowed an attacker to manipulate various vehicle functions, including killing the engine. Miller and Valasec famously demonstrated the hack on a vehicle in motion operated by Wired reporter Andy Greenberg in 2015.[15] The manufacturer of the Jeep, Chrysler, issued a safety recall for the Jeep and other vehicles with the same headunit; the fix was a software patch that had to be installed at an authorized dealership.

Automobile cybersecurity has improved somewhat since these and other instances of vehicle hacks. For example, after the Jeep hack, it is now standard practice for OEMs to put firewalls between the headunit and the CAN to reduce the risk that an attacker who has compromised the headunit is able to access and manipulate packets on the CAN.

Still, major security problems continue to emerge. In January 2023, for example, a team of researchers identified dozens of vulnerabilities spanning 18 car brands.[16] And attacks against OEMs' telematics and other backend infrastructures are on the rise, according to Upstream Security, which tracks cybersecurity incidents affecting the transportation sector, because the OEMs are becoming more reliant upon this infrastructure to deliver services.[17] We elaborate on the continued security problems of OEMs later in this paper.

Problems with the Gatekeeper Model and The Need for a New Approach to Data Governance

Traditionally, vehicle owners owned the data about their cars, which they could use for maintenance or other purposes. However, one approach that is being advanced to address cybersecurity risks in automobiles is to largely allow only the OEM to communicate directly with the vehicle. Vehicle occupants might still connect to the headunit with their smart devices, but all other communications to and from the vehicle would be with the OEMs or otherwise managed by them. Under this model, the vehicle owner might still own the vehicle's data (a principle OEMs sometimes dispute), but the OEMs would control access to vehicle data, making it available to vehicle owners only pursuant to contracts governing what data is shared and how it is shared. The vehicle owner would have no ability to send remote commands to their vehicle. We refer to this approach as the gatekeeper model. The purported rationale for this gatekeeper model is that the best way to protect the vehicle against malicious cyber intrusions is to strictly limit who can access vehicle data, and especially who can communicate with the vehicle in a bi-directional manner.

We agree that security threats to autos are real and will probably grow. We disagree, however, with the rationale for the gatekeeper model. Instead, the connected car ecosystem demands a more sophisticated approach to data governance and risk management.

---

[15] Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway—with Me in It," *WIRED* (July 21, 2015), available at https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
[16] Sam Curry, "Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and More" (Jan 3. 2023), available at https://samcurry.net/web-hackers-vs-the-auto-industry/.
[17] Upstream, "Automotive Cyber Trend Report" (2023), available at https://info.upstream.auto/hubfs/Security_Report/H1-2023_Report/Upstream_H1-2023_Automotive_Cyber_Trend_Report.pdf.

Automobile Connectivity: An Increasingly Diverse Ecosystem Requires Data Access

As the automobile sector becomes ever more data-dependent and data-driven, a major question is how that connectivity should be governed: How can maximum corporate and societal value and maximum vehicle occupant satisfaction be drawn from connected automobiles while ensuring that data security and cybersecurity risks are identified, mitigated, and managed?

In the case of commercially-owned and shared-use vehicles, including car sharing, corporate fleets, rental cars, and government fleets, there are at least three parties with major interests in the data and the ability to use that data to improve safety, performance, and occupant satisfaction: the OEM, the fleet owner, and the vehicle's occupants (which, in the future, may not include a driver). The OEM's primary interests are in car safety: the OEM is responsible for defects in design and manufacturing. The OEM must have the ability to recall cars and, as the car becomes more software-defined, to deliver safety updates to the car without the need for a service station visit. OEMs also have a strong interest in using data to monitor vehicle and component performance with regards to safety and quality.

The fleet manager, however, has equally compelling interests, since the fleet manager is responsible for car maintenance and shares in the responsibility for driver safety–responsibilities that would be difficult if not impossible to fulfill if vehicle connectivity were under the sole control of OEMs. Drivers (and passengers) have a privacy interest in the data about their location, about in-car conversations, about video from in-car cameras, and about the other increasingly sensitive data available within the car and the types of inferences that can be drawn from that data. Whoever obtains personal data[18] from the car is bound by privacy and cybersecurity laws, including laws requiring consent for collection and limits on reuse and laws imposing an obligation to secure the data against loss or misuse.

In addition to these critical interests, OEMs and fleet managers have other interests in the data, including around efforts to enhance the occupant experience and expand profitability with added services, information and entertainment.

In addition to these three paramount parties (OEMs, fleet managers, and vehicle occupants), many other parties have an interest in data about the vehicle and the driver or driving patterns: insurance companies interested in safe driving and in the recovery of stolen vehicles, environmental protection authorities enforcing emission control standards, law enforcement agencies seeking to locate criminal suspects, component makers, dealers (including those in the resale market), repair shops, municipalities pursuing smart city goals of traffic management and road maintenance, managers of the growing infrastructure of electric charging stations, government agencies promoting electric car usage, and many others.

Consequently, we are already in a world where these multiple entities have legitimate interests in the data generated by automobiles and the underlying connectivity. And with the transition to electric vehicles and autonomous vehicles, the number of entities that can gain commercial and societal value from automotive connectivity will continue to grow.

In this environment, a gatekeeper model—the model preferred by the OEMs, placing them as the chokepoint in a vast and socially desirable ecosystem—is fundamentally inefficient. Moreover, it has no guarantee of serving the security interests that the OEMs cite as the justification for their approach. Indeed, the centralization of data sought by the OEMs poses its own risks to security and privacy. Instead, a decentralized model of data governance needs to be developed, which can simultaneously serve the needs of innovation *and* security.

[18] "Personal information" is defined under California law as "information that identifies, relates to, describes is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." California Civil Code §1798.140(o)(1).

The Centralized Model of Data Security is Outdated and Ill-suited to Ecosystems

There is a long-running debate over whether a given organization should centralize or decentralize its data.[19] This debate goes back at least half a century, before the commercialization of the internet and before the mobility revolution, with arguments for and against the centralized model.[20]

Centralized security architecture can simplify the management, enforcement, and auditing of security policies, as well as reduce the complexity and cost of the data infrastructure. However, it can also create a single point of failure, a performance bottleneck, and a target for attackers. Moreover, it can limit the flexibility and scalability of the network, as any changes or updates require approval and coordination from the central authority. On the other hand, a decentralized security architecture can increase the resilience, performance, and adaptability of the network. However, it can introduce other challenges and risks, such as inconsistency of security policies, as well as coordination and communication issues among the decentralized nodes.

Within the context of a single organization, there is no right or wrong answer.[21] Security experts agree that choosing between centralized and decentralized security architecture depends on various factors, such as the size, complexity, and dynamics of the network, the type and level of security threats, the availability and capability of security resources, and the organizational culture and governance.

However, the connected car does not exist just within the ambit of one organization. As explained above, the connected car operates within an ecosystem, in which multiple entities have legitimate interests in the data and the vehicle's overall connectivity. In that context, centralization is both unnecessary and counterproductive, in terms of security and in terms of the ongoing innovation aimed at creating new value and achieving societal benefits from the connected car.

As analysts from PWC concluded:

> As more software is integrated into vehicles, it is becoming clear that cybersecurity is no longer the sole responsibility of the auto OEM. With most vehicle manufacturers procuring software and related technology from third-party suppliers, cyber protection is now a shared imperative spanning the automotive ecosystem. Leveraging a robust approach to establish internal and external controls is essential to achieving automotive data security.[22]

Centralization is Not Necessary to Achieve Safety and Security: Consider Aviation

The airline industry surely has safety and cybersecurity concerns at least as serious as those of the automobile industry. Yet the aviation sector has not pursued a gatekeeper model for governance of the data generated by airplanes. Instead, it has developed an ecosystem based on multiple, multi-directional data flows, which in turn has generated an environment of competition, collaboration, and innovation. As a senior officer of a leading jet engine maker, Rolls-Royce, said, the ecosystem is

[19] Alex Woodie, "To Centralize or Not to Centralize Your Data–That Is the Question," *datanami* (July 14, 2020), available at https://www.datanami.com/2020/07/14/to-centralize-or-not-to-centralize-your-data-that-is-the-question/.
[20] See Rein Turn, Norman Shapiro, M. L. Juncosa, "Privacy and Security in Centralized vs. Decentralized Databank Systems," *RAND Corporation* (1975), available at https://www.rand.org/pubs/papers/P5346.html.
[21] Lee Atchison, "3 Important Reasons Why You Shouldn't Centralize Your Data" (May 18, 2023), at https://leeatchison.com/app-architectures/reasons-you-should-not-centralize-data/; http://ccl.cse.nd.edu/research/papers/cons-sisw05.pdf.
[22] Akshay Singh et al, "Turbocharging Innovation Through Automotive Software," *PWC* (March 8, 2023), available at https://www.pwc.com/us/en/industries/industrial-products/library/automotive-software-trends.html.

based on the premise that "the airline is in control of that data, because they own it, they decide how they share it and whom they share it with."[23]

We examine here the data governance practices of the aviation sector solely in terms of what it tells us about the cybersecurity of telematics and other sensor data coming from a complex platform (whether an airplane or an automobile) where safety and reliability are essential. In cybersecurity terms, the bottom-line lesson from the aviation sector is that the gatekeeper model is unnecessary from a cybersecurity perspective.[24]

In the airline industry, at least three entities have direct access to data from airplanes: the aircraft operator (the airline, comparable to a fleet owner), the aircraft manufacturer, and the engine manufacturer. All three (owners, airplane assemblers, and engine manufacturers) receive data directly from the aircraft.[25] A fourth important participant in the data ecosystem is the provider of maintenance, repair, and overhaul (MRO) services.

Newer planes are providing airlines (the owners of the aircraft) with an even larger stream of data, which the airlines use for a wide range of purposes related both to safety and to the provision of added services intended to generate additional revenue streams.[26]

At the same time, the engine manufacturers have direct access to data from sensors on the engine. Until recently, the data from engines was only downloaded after the aircraft had landed, although alert messages indicating anomalies were able to be instantly transmitted to the engine manufacturer in-flight if particular parameters were exceeded. In the next phase of development, the data was accumulated and transmitted at regular intervals to ground stations monitored by the engine manufacturers. Most recently, as connectivity technology advances, it has become possible for engine manufacturers to receive and analyze continuous engine operational data (CEOD) in real time generated from engines in flight. For example, according

[23] Ekaterina Vuorinen, "Case Study: Rolls-Royce and Qoco - Working Together for PLM," *Qoco* (February 22, 2022), available at https://www.qoco.aero/blog/case-study-rolls-royce-and-qoco-working-together-for-plm. See also Martin Gubisch, "How MROs Respond to OEM Aftermarket Ambitions," Flight Global (Nov. 27, 2018) ("Airbus and Boeing have repeatedly said that airlines own the data that is generated during their operations."). Other participants in the sector agree that airlines own and control the data about their airplanes. For example, Collins Aerospace, a major manufacturer of airplane components, offers a service to airlines that can analyze data from Collins components on aircraft to predict future maintenance needs and otherwise support fleet management. Collins Aerospace, Analytic Services, https://www.collinsaerospace.com/what-we-do/industries/commercial-aviation/analytics-solutions/ascentia-analytics-services. Collins, like Rolls Royce, starts from the premise that the data about Collins components belongs to the airline: "We believe that each airline owns their own data and we want our users to have unrestricted access to it. Rather than stand in an airline's way, we want to enable users to do more with predictive maintenance." "Turning data into intelligence: Predictive maintenance," *Aviation Business News* (Dec. 24, 2022), available at https://www.aviationbusinessnews.com/mro/latest-news-mro/turning-data-into-intelligence-predictive-maintenance/. Another major player is SITA, whose e-Aircraft DataHub collects raw data from the airlines and then classifies, decodes, and distributes appropriate structured data sets to partners specified by the airline. SITA, e-Aircraft DataHub, https://www.sita.aero/solutions/sita-for-aircraft/data-and-platforms/e-aircraft-datahub/. "Airlines can choose when and how this aircraft data is used. It can either be packaged up and routed to the ground for later use, or it can be processed directly on the aircraft for pilot or crew applications." Marek Rakowski, "Aircraft data management for the future," *SITA* (Aug. 18, 2020) https://www.sita.aero/pressroom/blog/aircraft-data-management-for-the-future/. This is not to say that the issues surrounding data ownership are uncontested. See Leo Barnier, "Data ownership, an issue that is still far from being resolved," Le Journal de l'Aviation (Oct. 31, 2018) available at https://www.journal-aviation.com/en/news/41356-data-ownership-an-issue-that-is-still-far-from-being-resolved ("aircraft manufacturers are doggedly claiming direct ownership of data"). However, even where data *ownership* is contested, the airline industry is not based on a data gatekeeper model.

[24] Developments in data access in the aviation sector seem to be driven by economic competition, as manufacturers seek to claim a larger share of the very profitable aftermarket business of maintenance, repair, and overhaul (MRO), threatening the traditional role of independent MRO providers. Martin Gubisch, "How MROs Respond to OEM Aftermarket Ambitions," Flight Global (Nov. 27, 2018), available at https://www.flightglobal.com/analysis/analysis-how-mros-respond-to-oem-aftermarket-ambitions/130290.article.

[25] Tom Hedges, "Harvesting and Utilising the Vast Amounts of Data Produced by Modern Aircraft – Part 1," *Commsoft* (March 17, 2023), available at https://www.oases.aero/blog/harvesting-and-utilising-the-vast-amounts-of-data-produced-by-modern-aircraft-part-1/.

[26] Christine Negroni, "Newer Planes Are Providing Airlines a Trove of Useful Data," *The New York Times* (April 20, 2021), available at https://www.nytimes.com/2021/04/20/business/airplanes-technology-data.html.

to Rolls-Royce's website, aircraft engine data is transmitted to Rolls-Royce via satellite feed.[27] This new ability to analyze live data streams enables engine monitoring systems to become more proactive and predict problems before they actually happen.[28]

In addition, the airplane manufacturers collect data directly from aircraft.[29] This data flows from the airplane to the plane manufacturers who share this data with the operators in real time.[30] For example, Airbus Real Time Health Monitoring (AiRTHM) is an advanced service through which operators receive guidance on optimized maintenance and real-time troubleshooting. The uplink technology allows real-time remote access to aircraft data via a digital datalink system, enabling Airbus engineers to deliver maintenance and technical advice both in flight and on the ground. Airlines' use of these services, however, is discretionary, not mandatory; OEMs compete with independent third-parties in offering data-enhanced preventative maintenance and other decision support services.

Data flows are multi-directional. Some data flows from airlines to OEMs.[31] Other data flows from airlines to engine manufacturers. For example, Rolls-Royce collects data not only from its own sensors on the engine but also from the operators.[32] And airlines collect data directly from their own aircraft, using the Aircraft Interface Device (AID).[33]

The flows of data in the aviation sector are complicated and evolving. But that is our point: the remarkably complex, distributed, and collaborative data architecture in the airline industry shows that there is nothing pre-ordained and nothing necessary in an OEM-centric or gatekeeper model in safety-critical ecosystems.

Looking beyond aviation, data centralization has not been adopted for other data-rich platforms that also face security challenges, notably personal computers and cellphones. There are multiple entities with interest in data about the performance and use of these devices: the device OEM, the developer of the operating system, the makers of apps that can be added to the device, and the communications service provider. While all these participants can draw data directly from the device, none of them claims the right to centralized control over the data and none of them seeks to deny device owners the technical or legal ability to draw any and all data directly from the device. Indeed, especially for enterprise users, the security of internet-connected computers and mobile devices is based on the ability and responsibility of the device owner to directly monitor any and all data to or from its device.

The OEMs Have a Poor Record on Data Security and Privacy

Centralized data storage poses serious risks to privacy and data security. A September 2023 study by researchers at the Mozilla Foundation concluded that "The car brands we researched are terrible at privacy and security."

---

[27] John Goglia, "Aircraft Engine Monitoring: How It Works And How It Could Help Malaysia Air 370 Crash Investigators," *Forbes* (March 13, 2014), available at https://www.forbes.com/sites/johngoglia/2014/03/13/aircraft-engine-monitoring-how-it-works-and-how-it-could-help-malaysia-air-370-crash-investigtors/?sh=4db6dbfb7620.
[28] Bill Read, "Digital Takeover," *Royal Aeronautical Society* (March 20, 2018), available at https://www.aerosociety.com/news/digital-takeover/.
[29] John B. Maggiore, "Remote Management of Real-Time Airplane Data" (2007), available at http://www.lb.boeing.com/commercial/aeromagazine/articles/qtr_3_07/AERO_Q307_article4.pdf.
[30] See, for example, Boeing Airplane Health Management, https://services.boeing.com/maintenance-engineering/maintenance-optimization/airplane-health-management-ahm.
[31] SITA, "SITA Aircraft DataSuite for OEMs: Achieve More, with Real-Time Aircraft Data," *SITA for Aircraft* (2023), available at https://www.sita.aero/globalassets/docs/brochures/sita-for-aircraft-data-suite-oems_brochure.pdf.
[32] Anna Townsend, "Case study: IFS and Rolls-Royce connect the automated data pipeline," *Plant Services* (November 30, 2023), available at https://www.plantservices.com/technology/artificial-intelligence/article/33015653/case-study-ifs-and-rolls-royce-connect-the-automated-data-pipeline (describing the "back-and-forth flow of real-time data" between Rolls-Royce and aircraft operators).
[33] AIDs are made by third parties, Henry Canaday "American Airlines Installing Collins Device To Aid Predictive Maintenance," Aviation Week (April 26, 2023), but also by OEMs, such as Boeing, which sells AIDs to airlines to facilitate their direct download of data from Boeing aircraft, https://www.boeing.com/content/dam/boeing/boeingdotcom/features/innovation-quarterly/2023/11/direct-connection-aid.pdf.

Indeed the report concluded that automobiles were the "worst category of products for privacy that we have ever reviewed." The researchers were unable to obtain from any of the 25 brands even basic information about their security standards.[34]

The OEMs are burdened with an outmoded data architecture of their own making. As noted above, CAN protocol at the heart of the OEMs' design is notoriously vulnerable to compromise, lacking in basic encryption and authentication controls. On top of that, the complexity of the in-car electronics increases the threat. For decades, the typical system inside a car has consisted of multiple electronic control units (ECUs) each controlling a different part of the vehicle. A 2022 CapGemini study found that 93% of OEMs still have this traditional vehicle architecture, with independent controls for each vehicle function.[35] Any one of these independent functions may use millions of lines of code, presenting a substantial attack surface. For example, research from the Volvo Car Group revealed that an average Volvo vehicle in 2020 had 100 million lines of code, with this expected to grow tenfold in the next ten years.[36] For comparison, a passenger airplane has only around 15 million lines of code.[37]

According to analysts at PWC, the auto industry "has yet to fully integrate software as a core competency, often outsourcing to fill this gap, especially in software R&D. … Moreover, coding in the industry has yet to fully adopt leading practices, leaving many auto companies with monolithic architecture and designs that can bog them down with complexity and waste."[38]

This architecture, characterized by high volumes of software code, validation complexity, and supply chain risk, poses serious cybersecurity risks.[39] Yet only 10% of OEMs, on average, believe that they are well prepared to implement various cybersecurity measures, according to a 2022 CapGemini study.[40] Over a third (37%) of OEMs do not collect any data related to vehicle cybersecurity and out of those who do collect data, 25% do not analyze it to uncover patterns and insights.[41]

The Connected Car Ecosystem Requires a New Approach to Connectivity, Data Governance and Cybersecurity Risk Management

Centralization is not the only way to manage security risks associated with connectivity and data, and centralization is unnecessary for cybersecurity or privacy protection. Instead, both OEMs and fleet managers, along with their suppliers and partners, need to commit to a set of data governance practices suited to a decentralized connected car ecosystem. These include adopting a risk-based and threat-informed approach to security design and decision making, agreeing on clear practices around driver and/or occupant consent and secondary uses of data, applying the principle of defense in depth to security policies and controls, implementing data encryption and attack-resistant methods of authentication, and undertaking continuous monitoring, testing, and improvement of the security architecture. Above all, this will require collaboration, not centralization. As McKinsey concluded, "Collaboration among multiple players within the ecosystem will be necessary to capture full value."[42]

---

[34] Jen Caltrider, Misha Rykov and Zoë MacDonald, "It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy," *Mozilla Foundation* (Sept. 6, 2023), available at https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/.
[35] Alexandre Audoin et al, "Next Destination: Software," *Capgemini Research Institute* (2021), available at https://www.capgemini.com/wp-content/uploads/2022/02/Next-Destination-Software-_WEB.pdf.
[36] Id., p. 34.
[37] "Vehicle Cybersecurity: Control the Code, Control the Road," *Vehicle Dynamics International* (March 18, 2020), available at https://www.vehicledynamicsinternational.com/features/vehicle-cybersecurity-control-the-code-control-the-road.html.
[38] Singh et al (2023), note 22 above.
[39] Singh et al (2023), note 22 above.
[40] Alexandre Audoin et al (2021), note 35 above, at p. 29.
[41] Alexandre Audoin et al (2021), note 35 above.
[42] Michele Bertoncello et al, "Unlocking the Full Life-Cycle Value From Connected Car Data," McKinsey & Company (February 11, 2021), available at https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/unlocking-the-full-life-cycle-value-from-connected-car-data.

A key element of the governance model for decentralized data access and use is to realize that different entities in the ecosystem will have need for different data elements. There are important distinctions among data that is necessary to ensure proper vehicle function, data that relates to the owner's maintenance responsibility, data related to safety upgrades that are the responsibility of the OEM, and data that may be used to enhance the driver's comfort or experience. There are also important distinctions between data that needs to be personally identifiable versus data that can be used in anonymized or aggregated form.

Related to the concept of distinguishing among data elements is another cybersecurity concept: "separation of privilege." Within the automobile, this principle of cybersecurity means that access to and control of certain systems (e.g. infotainment and braking system) is separated, such that compromise of one does not compromise the whole network. OEMs can enhance the cybersecurity of their vehicles by integrating this concept into their data architecture.

Fleet Managers Have Powerful Incentives to Protect the Cybersecurity of Their Cars

Security shortcomings emerge when actors making decisions about security risk don't bear the full costs of their risk decisions. That is not the case here: fleet operators have strong incentives to ensure that the cars they are providing to their customers are safe and reliable. The fleet operator's customers expect the fleet operator to furnish cars that are safe and reliable. When a car does suffer a safety or reliability problem through no fault of the driver, the driver expects that the fleet operator will take ownership of the problem and fix it, even if the cause of the incident was not the fleet owner's fault.

The fleet operator faces an array of substantial direct and indirect costs as a result. Direct costs include provisioning an alternative vehicle for a customer, making repairs, foregoing revenue as a result of the downtime associated with restoring the vehicle to roadworthiness, and possibly a diminishment of the car's resale value. Indirect costs include potential reputational harms associated with the driver having a suboptimal experience.

All of these costs provide a powerful incentive to fleet managers to take cybersecurity seriously and undermine arguments that direct fleet owner access to certain data would open security flaws.

Risk management is about balancing risk. Accordingly, proposals made in the name of cybersecurity must be assessed in terms of both their benefits and their costs. In this case, the security case for the gatekeeper model is weak. On top of that, the proposal would result in harms to competition and innovation by allocating a windfall of negotiating leverage to the OEMs.

Conclusion

The connected car is already here, and further innovations promise a future of safer, more reliable, and more enjoyable driving experiences. Cybersecurity innovation must keep pace, and history and experience have shown that the gatekeeper model falls short. It is completely within the power of the OEMs to build into their cars security protections that would support a decentralized data architecture and the innovation it will enable. Indeed, without security protections to the OBD-II port, the OEM's in-car cellular uplink, and other features and interfaces, automobiles will remain vulnerable even if the data they generate were centralized.