Hypothesis

Security and Privacy Analysis on Personal Identifiable Informationfor Connected Commercial Vehicles

Jason Carlton *

Posted Date: 27 September 2024

doi: 10.20944/preprints202409.2195.v1

Keywords: Connected Vehicles; Data Privacy; Data Security; Infotainment System; Personal Identifiable Information; Ride-Sharing; Software; Technology; Rental Vehicles

Hypothesis

Security and Privacy Analysis on Personal Identifiable Information for Connected Commercial Vehicles

Jason Carlton

University of Michigan-Dearborn; jcarlto@umich.edu

Abstract: With many Americans eager to resume travel after prolonged restrictions from the coronavirus pandemic, car rentals are on the rise. According to Auto Rental News, "2021 U.S. Car Rental Revenue Climbs 21% Year-Over-Year" (Brown, 2021). In conjunction with increased car rental, and associated travel, we can expect to see an increase in cyber security and data privacy attacks. In the digital age, enterprises have a responsibility to protect consumers' personally identifiable information (PII). As it pertains to rental vehicles, when consumers connect their mobile devices to a rental vehicle's Entertainment and Infotainment System or utilize the built-in navigation feature, they do so, unbeknownst to themselves that the information from their devices is transferring to the vehicle, where it will remain, unless properly expunged from the system. A large majority of consumers are blissfully unaware that their PII is being stored, and how easy it would be for an adversary to potentially breach their data security and privacy. To expand upon this hypothesis, I conducted a further investigation on the subject, by partaking in the rental of three different vehicles, each belonging to a different manufacturer (Nissan, Chrysler, and Maserati), from three different vehicle rental companies (Enterprise, Hertz and Turo). I then, as a consumer, tested my hypothesis to determine if, I was able to easily breach the prior consumers' data security and privacy by viewing devices that had previously connected to the vehicle, as well as any of the previous consumers' personal information. The results were undeniable; the PII of the previous consumers is not protected.

Keywords: connected vehicles; data privacy; data security; infotainment system; personal identifiable information; ride-sharing; software; technology; rental vehicles

---

The Consumer Experience

Throughout the paper, as I reference my research, I will do so as Case A (Enterprise, Nissan), Case B (Hertz, Chrysler) and Case C (Turo, Maserati). To commence the investigation, I began by utilizing the Internet to reserve vehicles for Cases A and B, while utilizing an iPhone App, to reserve a vehicle for Case C. The reservation process in all three cases was very similar in terms of selecting a timeframe and providing a payment method for the rental.

At the time of vehicle inception, my experience varied slightly from Cases A and B to Case C. Cases A and B are what one would refer to as a traditional rental experience. For both of said cases a driver's license and credit card were required at the time of pick up. In addition, a representative from the rental agency visually inspected the vehicle, documenting notes prior to my departure. In Case C, all the personal details were handled through the App, including the inspection, in which both the owner of the vehicle and the renter are required to upload photos from the vehicle into the app.

In all three Cases (A, B and C), an inherent deficiency of the rental process was the lack of explanation to the privacy policy and or procedures. Neither during the pickup or drop off process, was there a mention of personally identifiable information that may or may not have been transferred to and left on the vehicle's computer. A traditional consumer, might assume, that data from their devices, is not stored on the vehicle, or if it is somehow transferred to the vehicle, such data would be cleaned, when the car is returned and prepared for the next renter. While it is possible that the

 doi:10.20944/preprints202409.2195.v1

employees and representatives of the rental agencies may not be aware of the data's existence, or of their own data privacy policies, lack of explanation of such a breach could impact how consumers use technology in vehicles, thus in many cases prompting renters to clean their own data prior to returning the vehicle.

The Data from Previous Consumers

Beginning my investigative work, with Case A, a lack of data privacy was evident, when upon entering and starting the vehicle a message promptly appeared on the vehicle's Infotainment screen stating, that it was trying to connect to the previous renter's iPhone. Immediately, I was able to go into the Infotainment system, through the settings and view all the prior renters' profiles, both Bluetooth and IOS. From what I could see, none of the previous renters' information had ever been deleted, as I was able to view data going back two years. Following a similar process with the other two rentals, it is to be noted that Case B followed suit with case A, providing both Bluetooth and IOS profiles, whereas Case C, only showed the Bluetooth profiles.

In both Cases A and B, where I was able to view the IOS profiles, I was not able to interact with or obtain any data from these profiles other than device name. The reason for this being, the devices that had been used were connected to the vehicle via USB, which kept the data stored on the phone and did not transfer the information to the car for easy access. This, however, does not mean that there is not data available on the vehicle's computer, as when a user does connect to the Infotainment system, via the USB, there is a prompt asking the consumer to download their device information, such as contacts, phone log, GPS history, etc. which are synched to one of the cars internal network/storage systems for the hands-free user experience.

When pertaining to information available in the vehicles from Bluetooth, all three cases A, B and C listed the profiles of all the mobile devices that previously paired to the vehicle. Bluetooth paired devices, like IOS, also download the same type of data to the vehicle, such as contacts, phone log, GPS, history, etc. which is used again for the same hands-free user experience. The main and most notable difference between Bluetooth and IOS, is that the data from the Bluetooth devices, was stored directly into the vehicles Infotainment system/computer and was readily available to anyone who had access to the car.

Vehicle Navigation Systems store synched data from both attached mobile devices (via Bluetooth or USB) and manually entered searches. In all three cases, (A, B and C), I was able to view locations that had previously been searched and located in the system. From there, it was simple to take this information and look up the addresses on the Internet to find out the names, property value, associated family members, etc.

It doesn't stop there. As ride sharing and rental apps are becoming increasingly more popular, so are crimes against the vehicle owners. According to the Washington Post, "Thieves are using peer-to-peer car rental apps to find their next ride." (Lazo, 2020), by creating a simple profile, searching for a vehicle, and finding that the keys are usually in the vehicle. Once in the vehicles, the thieves then have access to any PII data that was also left on the car.

Data Privacy Policies

With all three rentals, Cases A, B and C, I was not provided a privacy policy per say. What I was provided was a link in the online rental agreement, that took me to a privacy policy, where for all three, I had to dig to find the specifics regarding the handling of PII associated with the Infotainment system. Case A was the only rental company to specifically call out the use of data associated with Infotainment Systems and Vehicle Manufacturer Apps. Stating, "If you pair a mobile device with our vehicles' navigation or infotainment systems and choose to use OnStar, Apple CarPlay, Android Auto or other similar third-party software or services on the vehicle, personal information and other data may be transferred from the mobile device and stored on these systems. We cannot guarantee the privacy or confidentiality of such information. You should delete all such personal information and other data from these systems before the vehicle is returned to avoid subsequent occupants of the vehicle accessing this information." (Inc., 2022)

 doi:10.20944/preprints202409.2195.v1

For both Cases B and C, the privacy policy was broad and generic without a specifically mentioning Infotainment systems and the associated apps. Interestingly, none of the three-mention information related to secured end to end connections (e.g., integrity, authentication, etc.) while using the vehicle.

Conclusions/Recommendations

A large majority of consumers are blissfully unaware that their PII is being stored, and how easy it would be for an adversary to potentially breach their data security and privacy. Throughout my investigation, PII was retrieved from all three research Cases A, B and C. That data was then used to track down specific peoples' names, addresses, etc. on the Internet. According to USA Today, "Privacy International rented cars from Enterprise, Hertz, Zipcar and Europcar. In every case, personal data from previous users was stored on the Infotainment systems" (Sanders, 2018). My study solidifies that previous research and concludes that the PII of the previous renters is not protected. Rental companies' privacy policies are vague and lacking in relevant information consumers need to know and understand the vulnerability of data left in Infotainment systems, with no information related to the security of end-to-end connections (e.g., integrity, authentication, etc.) while using the vehicle.

As illustrated through the research, there are three things that could help in securing the consumers PII data. First, rental companies must implement a stricter privacy policy. Second, with remnants of data being left on these vehicles, enterprises have the obligation to expunge the PII prior to renting the vehicle to someone else. Finally, the sales associates need to be trained to reference these privacy policies to consumers, to ensure that the consumers are informed on the companies' current policies and said expectations as it regards to the consumers' need to remove their own data (at this present time.) As it stands today, the data of consumers personal identifiable information is not safe nor protected, and best practices need to be established to do so.

References

1. Brown, C. (2021, 12 08). *Auto Rental News*. Retrieved from AutoRentalNews.com: https://www.autorentalnews.com/10157505/2021-u-s-car-rental-revenue-climbs-21-year-over-year.
2. Inc., E. H. (2022, 02 21). *Privacy Policy*. Retrieved from Enterprise Rent A Car: https://privacy.ehi.com/en-us/home/privacy-policy.html.
3. Lacroix, J. (2017). *Ontario Tech University.* Retrieved from https://ir.library.dc-uoit.ca/bitstream/10155/821/1/Lacroix_Jesse.pdf: http://hdl.handle.net/10155/821.
4. Lazo, L. (2020, 02 14). *Thieves are using peer-to-peer car rental apps to find their next ride*. Retrieved from The Washington Post: https://www.washingtonpost.com/local/trafficandcommuting/thieves-are-using-peer-to-peer-car-rental-apps-to-find-their-next-ride/2020/02/13/b84d8e16-49c0-11ea-9164-d3154ad8a5cd_story.html.
5. Sanders, R. L. (2018, 01 30). *Car Renters Beware Bluetooth Use Can Reveal Your Private Data*. Retrieved from USA Today: https://www.usatoday.com/story/money/cars/2018/01/30/car-renters-beware-bluetooth-use-can-reveal-your-private-data/1080225001/.