Article

Safeguarding Personal-Identifiable Information (PII) after Smartphone Pairing with Connected Vehicle

Jason W Carlton * and Hafiz Malik *

Posted Date: 3 September 2024

doi: 10.20944/preprints202409.0240.v1

Keywords: connected vehicles; connected vehicle architecture; data privacy; data security; infotainment system; personable identifiable information (pii); ride sharing; software; technology; rental vehicles

Article

Safeguarding Personal-Identifiable Information (PII) after Smartphone Pairing with Connected Vehicle

Jason Carlton * and Hafiz Malik *

Electrical Engineering Department, University of Michigan-Dearborn, Dearborn, MI 48128 USA
* Correspondence: jcarlto@umich.edu (J.C.); hafiz@umich.edu (H.M.)

Abstract: The integration of connected autonomous vehicles into the transportation system introduces significant enhancements in driving experience and convenience. Yet, it simultaneously raises important concerns regarding the security and privacy of passenger data. As individuals increasingly depend on these connected vehicles, particularly rental cars with advanced infotainment systems, safeguarding their personal information becomes a paramount imperative, presenting significant challenges that must be addressed to maintain user trust and comply with privacy regulations. This paper investigates risks associated with personal information stored in connected vehicle technology, emphasizing the importance of robust security and privacy practices. In the advent of cyber threats and the need for data protection, we examine a risk management framework (RMF) as suggested by NIST, which aims to address these quintessential concerns preemptively. Our research moves beyond the limitations of manual safeguarding methods, supporting the necessity for an advanced automated technical solution. To address these issues, we introduce and meticulously assess the efficacy of "Vehicle Inactive Profile Removal" (VIPR), an innovative technical solution conceived to actively eliminate the risks and potential oversights that stem from the prevalent tendency of renters to leave personal data unerased in the infotainment systems of rented connected vehicles. We provide a thorough evaluation of VIPR through various scenarios, including vehicle return to a rental depot, subsequent rentals, and ridesharing contexts. Our proof of concept includes an array of experiments to demonstrate how VIPR proficiently and autonomously removes previous renters' "Inactive" profiles from a simulated infotainment system. The results highlight how VIPR constitutes a critical step towards enhancing the privacy and security of personal data, thereby promoting a safer, more responsible use of connected vehicle technology in society.

Keywords: connected vehicles; connected vehicle architecture; data privacy; data security; infotainment system; personable identifiable information (pii); ride sharing; software; technology; rental vehicles

1. Introduction

As the Internet of Things (IoT) is becoming more integrated into our modern living, personal information security in devices ranging from connected autonomous vehicles (CAVs) to general smart gadgets has become a challenging task. The proliferation of these IoT and intelligent transportation systems ushers in a new era of convenience and efficiency, yet simultaneously poses a formidable challenge in protecting the troves of personal identifiable information (PII) they collect, store, and process. For instance, safeguarding personal information stored on infotainment systems after pairing smartphones remains a huge challenge for CAVs [1].

Through the continually advancing connectivity and autonomy in vehicles, PII protection becomes even more salient. In the realm of transportation, CAVs are rapidly transitioning from speculative innovation to tangible reality. The integration of CAVs within urban planning and public transportation systems suggests a future where interactions with PII extend beyond the personal scope into the public domain. The significance of holistic data management across such expansive networks is underscored by the anticipated saturation of CAVs in the market. Industry forecasts by CarBuzz shows a robust upward trend, with an estimated 15.5 million IoT-equipped vehicles, including CAVs, entering the US market in 2023 alone [2].

Through our recent study, we have noted that the vehicle rental market is more vulnerable to PII leakage due to lack of regulations and protocols to protect renters' PII after the vehicle is returned to the lender. A recent study reveals that in 2022, 2,111,921 vehicles were in service within the U.S. rental market, as depicted in Table 1. This number saw significant growth in 2023 to 2,263,900 vehicles that overall represents 15% of the population [3]. According to Peter Jones of *Motor and Wheels*, rental companies' average rental is in the range of 2 to 3 days [4] and typically retain their fleet for a span of two to four years [5], during which each vehicle accrues an average mileage ranging from 25,000 to 40,000 miles.

Table 1. 2022 U.S. Rental Vehicles in Service.

2022 U.S. Car Rental Market by Fleet, Locations, and Revenue				
Company	U.S. Cars in Service (Avg.) 2022	Number of U.S. Locations	2022 U.S. Revenue Est. (millions)	2021 U.S. Revenue (millions)
Enterprise Holdings (includes Alamo Rent A Car, Enterprise Rent-A-Car, National Car Rental)	1,200,000	5,500	19,915	15,664
Avis Budget Group (includes Payless, not Zipcar)	425,000	3,000	8,430	6,045
Hertz (includes Dollar & Thrifty)	365,000	3,900	5,700	5,600
Sixt	29,000	98	970	650
Fox Europcar	18,571	27	391	330
ACE Rent A Car	12,000	75	120	100
NP Auto Group (Priceless & NextCar)	7,350	101	62	50
Green Motion U-Save Group	8,500	84	40	33
Rent-A-Wreck of America	1,500	60	15	16
Independents	45,000	3,800	450	425
Totals	**2,111,921**	**16,645**	**36,093**	**28,913**

These vehicles, alongside other IoT devices, are equipped with various communication technologies such as Wi-Fi, LTE/5G, Dedicated Short Range Communications (DSRC), and Vehicle-to-Everything (V2X) communications, as shown in Figure 1 expanding their capabilities and complexity.

Traditional in-vehicular networks (VANETs) like Controller Area Network (CAN) network, Media-Oriented Systems Transport (MOST) network, Local Interconnected Network (LIN) network, FlexRay network (as shown in Figure 2), and automotive ethernet are now intertwined with advanced sensor fusion systems that's essential for autonomous driving, traffic management, and predictive maintenance. Similar networking structures are present in a wider range of IoT devices, forming a comprehensive mesh of interconnected smart systems with PII distributed at every node.

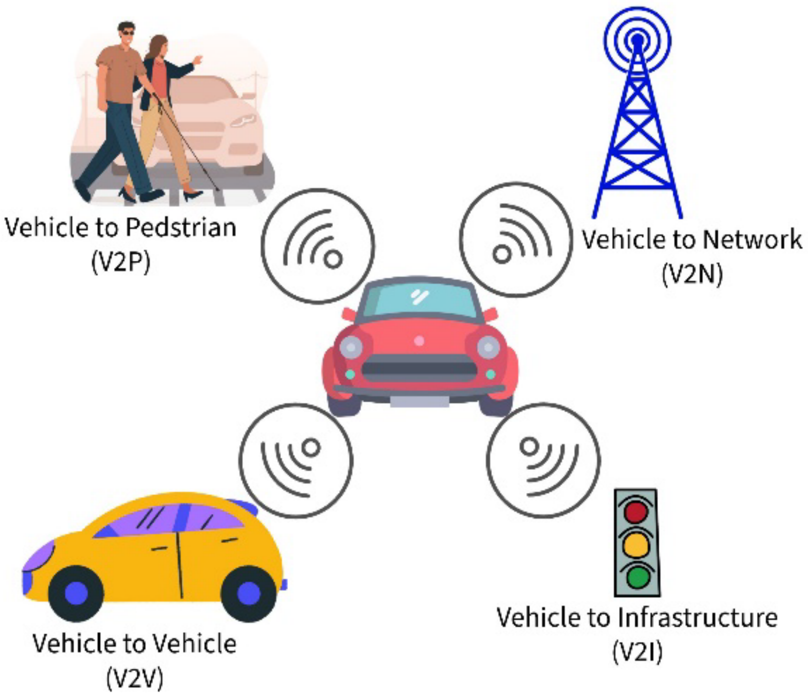


Figure 1. Illustration of Vehicle to Everything (V2X) Communications Model.

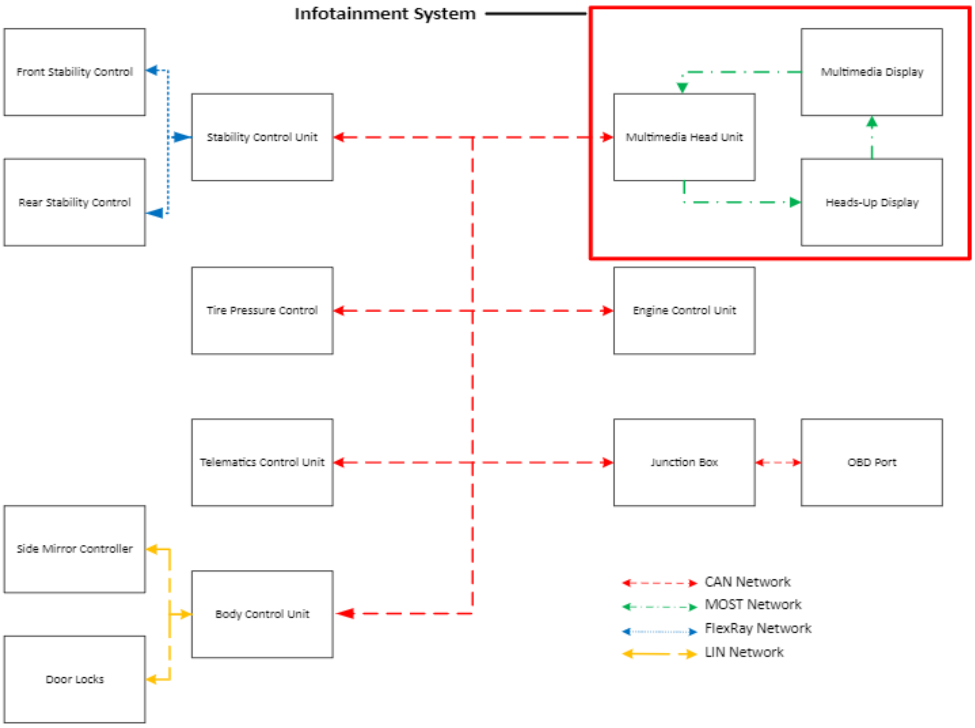


Figure 2. Illustration of Modern In-Vehicle Network Architecture.

Exposing PII at every node is a significant privacy risk, especially when pairing a mobile device to an infotainment system and when renters don’t properly expunge their information (please see Figure 3).

doi:10.20944/preprints202409.0240.v1

To illustrate the privacy leakage due to smartphone pairing with modern vehicles, we conducted a hands-on study to investigate whether *renters* leave their personal identifiable information (PII) on the rental vehicle infotainment systems [6]. Our research confirmed renters were leaving their PII on infotainment systems and is not protected for subsequent renters. To further investigate the PII leakage problem, we surveyed to assess public awareness concerning this problem [7]. The primary goal of the survey was to understand the importance consumers place on their personal information when considering the risk of it being left undeleted and subsequently shared with future renters. Specifically, we sought their perspectives on the potential consequences of leaving their PII on rental car infotainment systems. For this study, we sent a questionnaire to ~600 consumers with 120 responses who had prior rental experience. Most of the participants from that survey were unaware they needed to manually delete their PII before returning the rental vehicle. All participants were unanimous for an automated solution to perform the PII deletion task.

Inspired by the findings of these investigations, we proposed a framework to address PII leakage problem related to smartphone pairing. This paper is focused on the design and implementation of an automated technical solution called the Vehicle Inactive Profile Remover (VIPR). VIPR is an advanced technical solution that lists ALL paired profiles with the vehicle's Bluetooth stack, marking the renter profile performing the pairing as 'Active' and ALL others as 'Inactive.' Based on defined intervals, VIPR automatically expunges the PII of 'Inactive' profiles from the infotainment systems, ensuring the renters PII is removed. This process is illustrated at a high level in Figure 3.

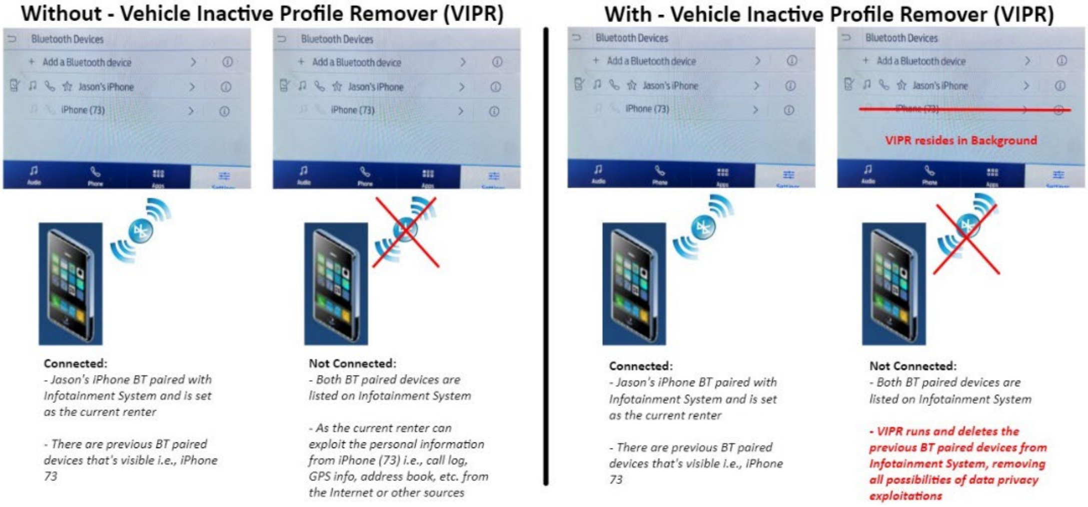

Without - Vehicle Inactive Profile Remover (VIPR)
With - Vehicle Inactive Profile Remover (VIPR)
Bluetooth Devices
+ Add a Bluetooth device
Jason's iPhone
iPhone (73)
~~iPhone (73)~~
VIPR resides in Background
Audio
Phone
Apps
Settings
Connected:
- Jason's iPhone BT paired with Infotainment System and is set as the current renter
- There are previous BT paired devices that's visible i.e., iPhone 73
Not Connected:
- Both BT paired devices are listed on Infotainment System
- As the current renter can exploit the personal information from iPhone (73) i.e., call log, GPS info, address book, etc. from the Internet or other sources
Connected:
- Jason's iPhone BT paired with Infotainment System and is set as the current renter
- There are previous BT paired devices that's visible i.e., iPhone 73
Not Connected:
- Both BT paired devices are listed on Infotainment System
- VIPR runs and deletes the previous BT paired devices from Infotainment System, removing all possibilities of data privacy exploitations

Figure 3. High-Level Illustration PII Leakage through Bluetooth Pairing and Removing User Profiles using VIPR.

The following sections illustrate the framework and functionality of VIPR, demonstrating its effectiveness in safeguarding PII in rental vehicles.

1. ***Comprehensive Review of PII Threats****: This paper systematically explores privacy risks specific to the IoT and connected autonomous transportation ecosystems, charting potential vulnerabilities and attack vectors.*
2. ***Privacy Impact Assessment:*** *A detailed study assesses the impact of PII breaches, emphasizing the unique challenges posed by CAVs and transportation systems, yielding insights into consumer awareness and behavior.*
3. ***Policy Evaluation:*** *An evaluation of existing privacy policies, highlighting gaps in current regulations and standards for emerging technologies in the IoT and CAV sectors.*
4. ***Development of a Universal Solution:*** *Introducing the Universal Inactive Profile Remover, a cross-sectoral technology designed to automate the erasure of PII from IoT devices, including all types of connected vehicles, creating a safer digital environment.*

5. ***Experimental Validation:*** *Experimental results demonstrate the effectiveness of the proposed solution in various scenarios, substantiating its application as a robust PII management tool.*
6. ***Future Directions:*** *A forward-looking discussion is offered, suggesting pathways for future research, the evolution of standards, and the potential integration of the proposed framework within broader IoT and transportation systems.*
7. ***Ethical and Social Considerations:*** *An analysis of the broader ethical and social implications of PII data management in IoT and autonomous transportation, promoting a dialogue on privacy and trust in an automated age.*

2. Related Work

The rapid integration of connected vehicle technology has significantly complicated the task of protecting consumer personal information within rental vehicles' infotainment systems. Despite heightened awareness and attempts to curb this escalating risk, the status quo continues to lean heavily on manual processes that place the onus of action squarely on consumers, a pattern underscored previously in this paper.

During our investigation for automated methodologies to reduce this risk, we scrutinized a variety of approaches. A particular highlight among these is Privacy4Cars [8], an application designed to guide consumers through the erasure of their personal data from vehicle infotainment systems. Nevertheless, our thorough testing of this application revealed that it falls short of an authentic automated solution, instead providing step-by-step manual instructions. While this service is initially offered without cost, it transitions to a paid subscription model after the trial period, which may deter sustained consumer engagement and adherence to data protection protocols.

Complementing these individual efforts, an FTC-led workshop addressing connected vehicle security convened a multifaceted group of experts, including original equipment manufacturer (OEM) executives, FTC commissioners, and consumer rights advocates [9]. This symposium addressed vital concerns regarding the preservation of consumer personal data, in addition to formulating security recommendations and exploring avenues for effective risk mitigation strategies. Critical outcomes included the recognition of the necessity for greater interoperability and information exchange among OEMs, the refinement of vehicle networking infrastructure, and the strategic implementation of risk assessment practices.

In a related vein, the Government Accountability Office (GAO) initiated an investigation analogous to that of the FTC workshop [10], requesting input from 16 OEMs about their data handling practices linked with connected vehicles. Out of the respondents, only 13 OEMs admitted to their role in collecting, using, and sharing various types of user data, highlighting operational and locational aspects. The GAO report reaffirmed the shared oversight responsibilities of the FTC and NHTSA in safeguarding consumer privacy and ensuring vehicle safety, underscoring the former's authority and activities in crafting consumer privacy guidelines, and facilitating educational workshops catered to the emerging concerns in the connected vehicle sector.

Drawing upon the lessons gleaned from the collective efforts of the FTC and GAO, OEMs are well-positioned to implement the National Institute of Standards and Technology's Risk Management Framework (NIST RMF) [11]. The RMF strongly advocates for the inception and sustained execution of comprehensive privacy programs that conform to established privacy laws and address the risks associated with PII processing. This framework is decidedly pertinent against the backdrop of software-centric modern vehicles, which introduce broader attack vectors and thus, greater opportunities for malicious entities to harness personal data.

An advanced adoption of the NIST RMF by OEMs would have been instrumental in cultivating an environment of proactive risk identification and mitigation. Comprehensive risk assessments conducted in advance of deploying connected vehicle technologies could have charted a course for the development of robust security measures. The RMF's structures model an industry-wide safeguard, potentially mitigating the emerging threat landscape by elevating the standards for information security in a pre-emptive manner. This anticipatory stance could have served as a bulwark against the sophistication of modern privacy threats, ensuring that consumer data is not only treated with the utmost care but also robustly defended against an array of cyber threats.

3. PII Leakage In the Car Rental Market

In January 2022, we initiated an investigative study, "Security and Privacy Analysis on Rental Vehicles: Assessing Potential Vulnerabilities to Consumers' Personal Identifiable Information (PII)" [6], which sought to build on existing research by analyzing the specific risks consumers face regarding the protection of personal information within a rental connected vehicle's infotainment systems.

The study involved the rental of three distinct vehicles from Hertz, Enterprise, and Turo, scrutinizing each for traces of PII left by previous renters. Our methodology included checking for devices that had been paired with the vehicle's systems via Bluetooth or Apple CarPlay and searching for any residual data that might disclose the identities of the vehicle's past users. The examination led to a concerning discovery: all three vehicles retained PII from past renters, ranging from contact lists to GPS locations and saved addresses.

This information laid bare the risks to which consumers are routinely exposed. Many renters remain unaware not only of the data stored during their use of the vehicle but also of the potential ease of access by unauthorized parties. During the rental process, we also noted a lack of explicit privacy instructions or guidelines informing customers of their responsibility to remove their PII before returning the vehicle.

The extent of PII retrievability was further tested by utilizing the data extracted from the infotainment systems to locate corresponding individual names, addresses, and additional information available on the internet. This exercise was in alignment with findings from a report by USA Today, which indicated similar concerns with the privacy policies of major rental companies like Enterprise, Hertz, Zipcar, and Europcar [1]. Every rented vehicle from these companies held onto personal data from its previous users.

Our study strengthens the argument that previous renters' PII needs to be more adequately protected, and there is a glaring deficiency in how rental companies communicate privacy policies. These policies are frequently buried within contracts and lack clarity, leaving consumers uninformed and unprepared to protect their privacy. Not only is the verbiage vague, but it also often omits essential details about the security measures safeguarding end-to-end connections, including the integrity and authentication protocols in place during the vehicle's operation.

The implications of our study are twofold: it reveals a widespread issue of data vulnerability in rental vehicles' infotainment systems, and it identifies a critical need for rental companies to be more transparent and proactive in educating consumers about these risks. The study advocates for industry-wide changes to ensure consumer data is consistently and effectively protected, including reforming privacy policy disclosures and introducing mandatory PII removal notifications for customers before vehicle return. These recommendations aim to mitigate the likelihood of inadvertent data exposure and enhance overall privacy standards within the rental vehicle industry.

4. Smartphone Pairing to Rented Vehicle: A Consumer Perspective

To build upon the insights gleaned from our independent study, we initiated a survey targeting a clearer understanding of renters' attitudes toward the risks associated with their personal information remaining on a rental vehicle's infotainment system after use. An illustrative article by Privacy International paints a picture of the issue: upon connecting a mobile device to a connected vehicle, the user encounters a list of names belonging to a variety of previously connected devices—phones like "Mike's iPhone" or nicknames such as "Bikerboy_Troi"—as well as potentially accessing navigation history that reveals the travel patterns of past users [12].

This surveilled sentiment was disseminated to 600 individuals via several social media avenues, including community groups on Facebook and professional networks like LinkedIn. From this outreach effort, we collected data from 120 participants. A significant portion of the participants, i.e., around 100 participants (83.3%), rated their personal information as highly important. It is important to note that only 67.5% of participants () showed varying degrees of tolerance on a scale from 1 to 5 on the question about the tradeoff between comfort level and their information being shared with subsequent renters, [13].

Diving deeper into users' behaviors revealed that 82 participants (68.3%) either admitted to a lapse in deleting their personal information from the infotainment system upon returning the rental or indicated uncertainty over whether this responsibility fell to them or the rental company. This confusion underscores a crucial gap in the communication and policies of rental companies regarding data privacy responsibilities.

Moreover, we identified a significant knowledge gap: 52% of survey respondents needed to learn or were unsure how to manually remove their personal data from the infotainment systems, an issue exacerbated by the rental agencies' lack of guidance or assistance.

Despite these disparities and uncertainties, there was unanimous consent among survey participants on one critical issue: the imperative for an automated solution that could address these privacy concerns. Such a solution would deliver a dual benefit—effortlessly protecting user privacy by eradicating left-behind personal data and granting peace of mind to consumers concerned about privacy in the digital age. By alleviating the burden of manual deletion, an automatic system could help transform the car rental experience, ensuring personal data is cleared without requiring specific action from the user, thereby preventing potential privacy breaches and establishing a new standard in protecting personal information within the rental car industry.

5. Proposed Framework to Safeguard PII in Rental Vehicles

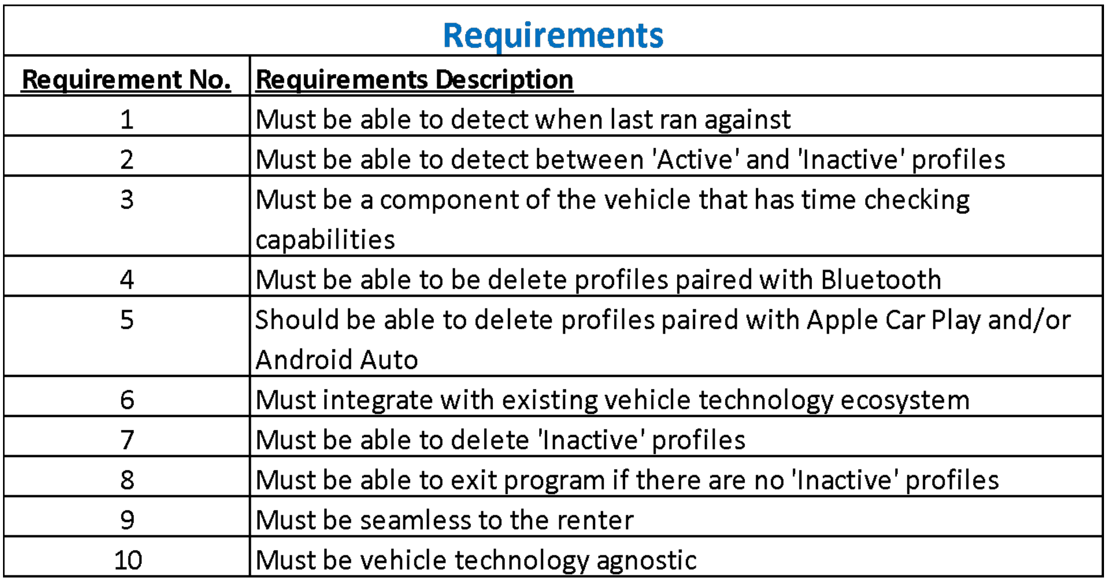
In response to our security and privacy analysis [7], we have proposed a robust solution called Vehicle Inactive Profile Remover (VIPR) that automatically removes personal identifiable information (PII) from the infotainment systems of rental vehicles with paired devices. VIPR is an advanced software-based solution that functions as a technological control framework designed to address the three key critical issues related to PII in rental vehicles.

1. ***Rental Vehicle Depot Return:*** *Emphasizes the importance of renters deleting their personal information before returning the rental vehicle.*
2. ***Subsequent Rentals:*** *This section highlights rental organizations' responsibility to delete renters' personally identifiable information before a subsequent rental.*
3. ***Ridesharing:*** *Introduces a scenario where, upon picking up and dropping off a rental vehicle at the exact location, the renter is prompted with a message on the infotainment display seeking consent to delete their personal information; otherwise, the profiles will be automatically removed.*

5.1. Framework Requirements

To effectively address the three key critical issues, we conducted extensive research to help us build a robust software-based solution. Our research, however, indicated a prevalent reliance on a manual process for deleting renters' personal information. Therefore, we developed a comprehensive set of requirements based on the findings from previous studies to ensure the effectiveness of VIPR. As shown in Table II, we identified ten key requirements that guided the analysis, design, and implementation phases of VIPR.

Table 2. Ten VIPR Foundational Requirements.



Requirements	
Requirement No.	**Requirements Description**
1	Must be able to detect when last ran against
2	Must be able to detect between 'Active' and 'Inactive' profiles
3	Must be a component of the vehicle that has time checking capabilities
4	Must be able to be delete profiles paired with Bluetooth
5	Should be able to delete profiles paired with Apple Car Play and/or Android Auto
6	Must integrate with existing vehicle technology ecosystem
7	Must be able to delete 'Inactive' profiles
8	Must be able to exit program if there are no 'Inactive' profiles
9	Must be seamless to the renter
10	Must be vehicle technology agnostic

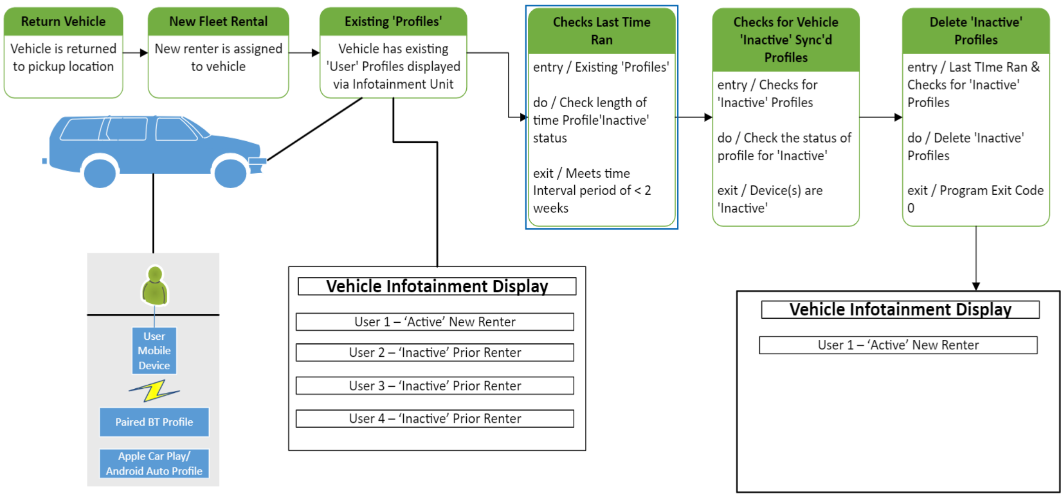
5.2. VIPR Analysis

After documenting essential requirements, the advanced solution we developed must seamlessly0 integrate into the existing in-vehicular network (IVN) architecture (as illustrated in Figure 3). To achieve this seamless integration, we analyzed the leading vehicle network controller area network (CAN) and all of its subsystems, i.e., the stability control unit and engine control units [14]. In our final analysis and to meet some of the core integration requirements, we designed our solution to utilize the vehicle's CAN, MOST, and LIN networks.

5.3. VIPR Design

In our design approach, we translated our key requirements and analysis into state diagrams to visually clarify our strategy to address these critical issues. As part of the rental depot and subsequent rental issue, we propose the following 6-step process (as shown in Figure 4).

1. ***Return Vehicle:*** *The current renter returns the rental vehicle to the depot, such as Enterprise, Hertz, or Turo.*
2. ***New Fleet Rental (Subsequent Renter):*** *After the rental is checked in at the depot and prepared by the rental organization for a subsequent renter.*
3. ***Existing "Profiles":*** *Pairing your mobile phone as a new renter to the vehicle and it has existing "User Profiles" displayed on the infotainment system.*
4. ***Checks Last Time Ran:*** *This is a time-based event that triggers on defined intervals i.e., every 30 seconds.*
5. ***Checks for Vehicle "Inactive" Synced Profiles:*** *This function checks the infotainment system for "Inactive" profiles.*
6. ***Deletes "Inactive" profiles:*** *At this step, the "Inactive" profiles are automatically deleted from the infotainment system.*


Return Vehicle
Vehicle is returned to pickup location
New Fleet Rental
New renter is assigned to vehicle
Existing 'Profiles'
Vehicle has existing 'User' Profiles displayed via Infotainment Unit
Checks Last Time Ran
entry / Existing 'Profiles'
do / Check length of time Profile'Inactive' status
exit / Meets time Interval period of < 2 weeks
Checks for Vehicle 'Inactive' Sync'd Profiles
entry / Checks for 'Inactive' Profiles
do / Check the status of profile for 'Inactive'
exit / Device(s) are 'Inactive'
Delete 'Inactive' Profiles
entry / Last TIme Ran & Checks for 'Inactive' Profiles
do / Delete 'Inactive' Profiles
exit / Program Exit Code 0
User Mobile Device
Paired BT Profile
Apple Car Play/ Android Auto Profile
Vehicle Infotainment Display
User 1 – 'Active' New Renter
User 2 – 'Inactive' Prior Renter
User 3 – 'Inactive' Prior Renter
User 4 – 'Inactive' Prior Renter
Vehicle Infotainment Display
User 1 – 'Active' New Renter

** 'Inactive' Profiles from Vehicle Automatically Deleted **

Figure 4. VIPR State Diagram for Rental Vehicle Depot Return & Subsequent Rentals.

Furthermore, we outlined a 3-step process to address the ridesharing issue, as shown in Figure 5. There is an additional capability in this process that allows the renter to select a "Delete Personal Information" button, which will display on the infotainment system when the vehicle is turned off at the exact drop-off location.

1. ***Pick-up Vehicle:*** *The rental vehicle is picked up from a remote location, such as a city street.*
2. ***Existing Pre-Defined Locations:*** *Check the infotainment system for "Inactive" profiles, i.e., previous renters' location histories, personal information, etc.*
3. ***Prompt on Infotainment Display:*** *Once the rental is completed, the vehicle is returned to the same location. When turned off, a prompt will be displayed on the infotainment system, allowing the renter to delete their personal information manually. If the renter decides to opt out, the program will still execute deletion at the established pre-defined time.*

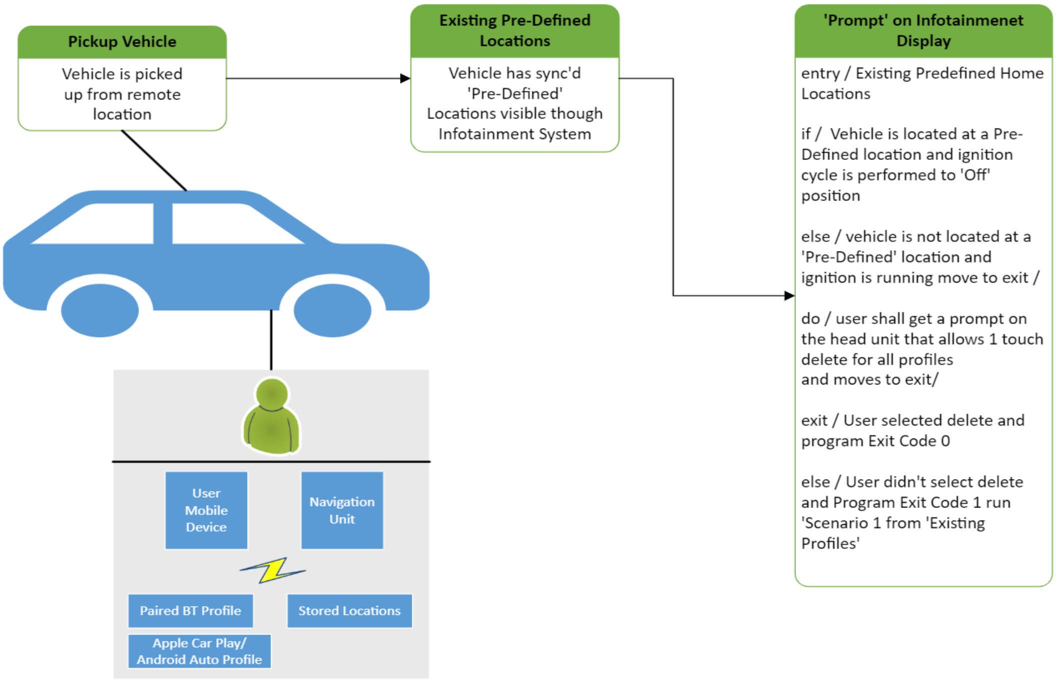

Pickup Vehicle
Vehicle is picked up from remote location
Existing Pre-Defined Locations
Vehicle has sync'd 'Pre-Defined' Locations visible though Infotainment System
'Prompt' on Infotainmenet Display
entry / Existing Predefined Home Locations
if / Vehicle is located at a Pre-Defined location and ignition cycle is performed to 'Off' position
else / vehicle is not located at a 'Pre-Defined' location and ignition is running move to exit /
do / user shall get a prompt on the head unit that allows 1 touch delete for all profiles and moves to exit/
exit / User selected delete and program Exit Code 0
else / User didn't select delete and Program Exit Code 1 run 'Scenario 1 from 'Existing Profiles'
User Mobile Device
Navigation Unit
Paired BT Profile
Stored Locations
Apple Car Play/ Android Auto Profile

Figure 5. VIPR State Diagram for Ridesharing.

6. VIPR Experiments and Results

To test our theory of the proposed framework, we established a laboratory environment equipped with a Raspberry Pi featuring Wi-Fi and Bluetooth capabilities and a 7-inch touchscreen display to emulate the interface of an infotainment system. We developed Python code that checked, validated, and deleted the "Inactive" profiles. This section will outline a series of experiments that validate our technical solution and proposed framework.

6.1. Experiement 1: Vehicle Infotainment System Replication

For this experiment, we wanted our 7-inch touchscreen display to accurately replicate the interface of an actual connected vehicle infotainment system, as shown in Figure 6.

6.2. Experiment 2: Collecting Paired Devices and their Status

In this experiment, the VIPR solution displayed a list of device profiles, including their respective states, on the 7-inch touchscreen infotainment system display. After clicking on the "**Paired**" button from the prior experiment, a list of device profiles and their real-time status was displayed that clearly distinguished between "**Active**" connections, shown as "**Yes**," and "**Inactive**" connections, displayed as "**No**." Figure 7 shows three profiles were created: two marked as "**Active**" and one as "**Inactive**." The "Inactive" profile would represent a prior renter's device in a rental vehicle infotainment system.

6.3. Experiment 3: Viewing Current and Previous Paired Devices

In this experiment, users could view the current and previously paired devices on the infotainment system by highlighting and clicking on the Bluetooth menu item, as shown in Figure 8. The green status button represents an **"Active"** paired device, indicating the current renter. The red status button indicates an **"Inactive"** paired device, which would be automatically deleted.

6.4. Experiment 4: VIPR Automatically Removing "Inactive" Profiles

For this experiment, we tested that VIPR removed the "Inactive" profile labeled as "**Sam's S10+**," as shown in Figure 9. The success of this experiment is evident with the profile no longer listed VIPRs effectiveness in automatically deleting inactive profiles.

6.5. Experiment 5: Checking "Active" Profiles After "Inactive" Profiles Deleted

In this final experiment, we tested current profiles in the infotainment system after executing Experiment 4—removal of inactive profiles. The remaining list of "Active" profiles in the VIPR system is shown in Figure 10. This figure shows the infotainment system currently paired devices only. This simulates the scenario of a current renter who paired their device to the rental vehicle.

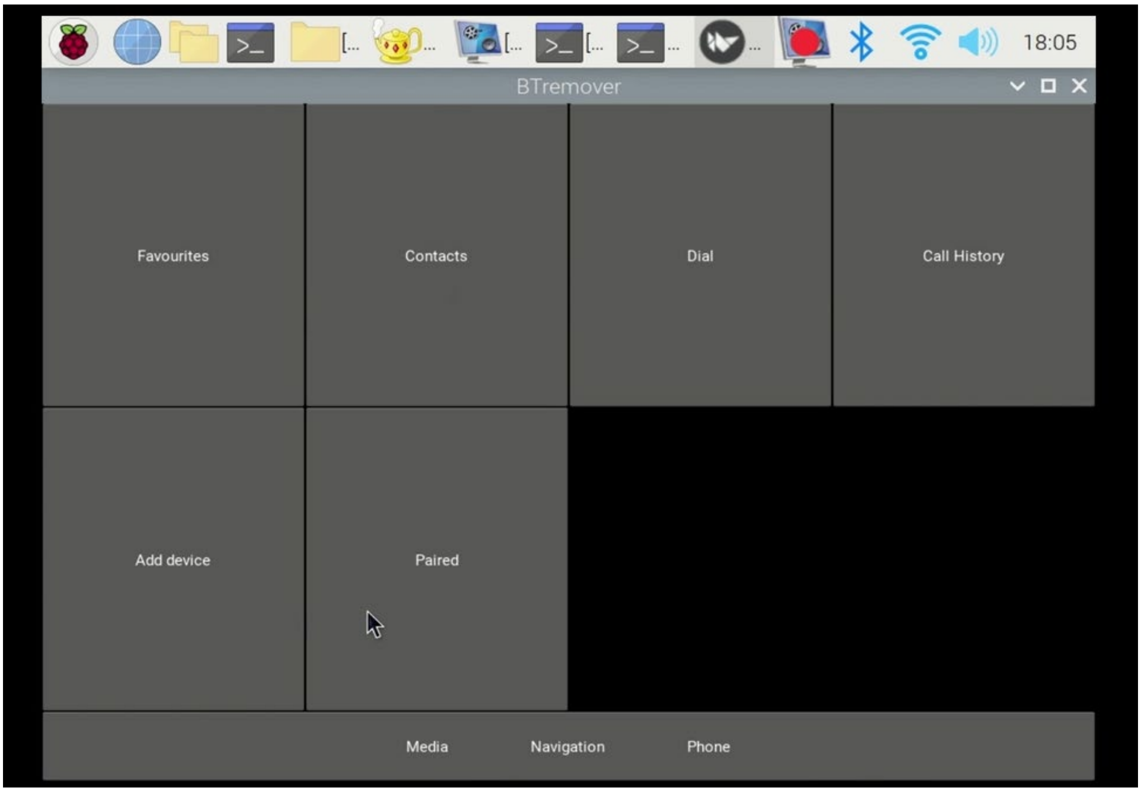
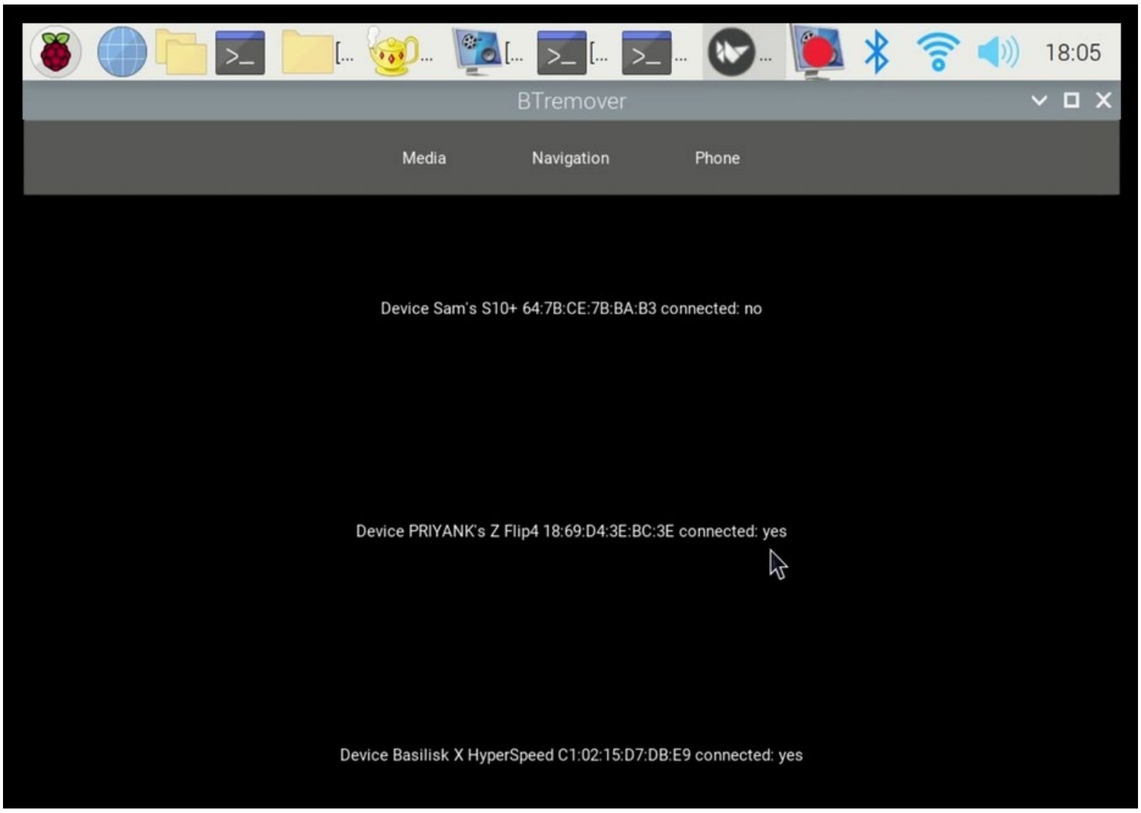


Figure 6. Replicated Vehicles Infotainment System.

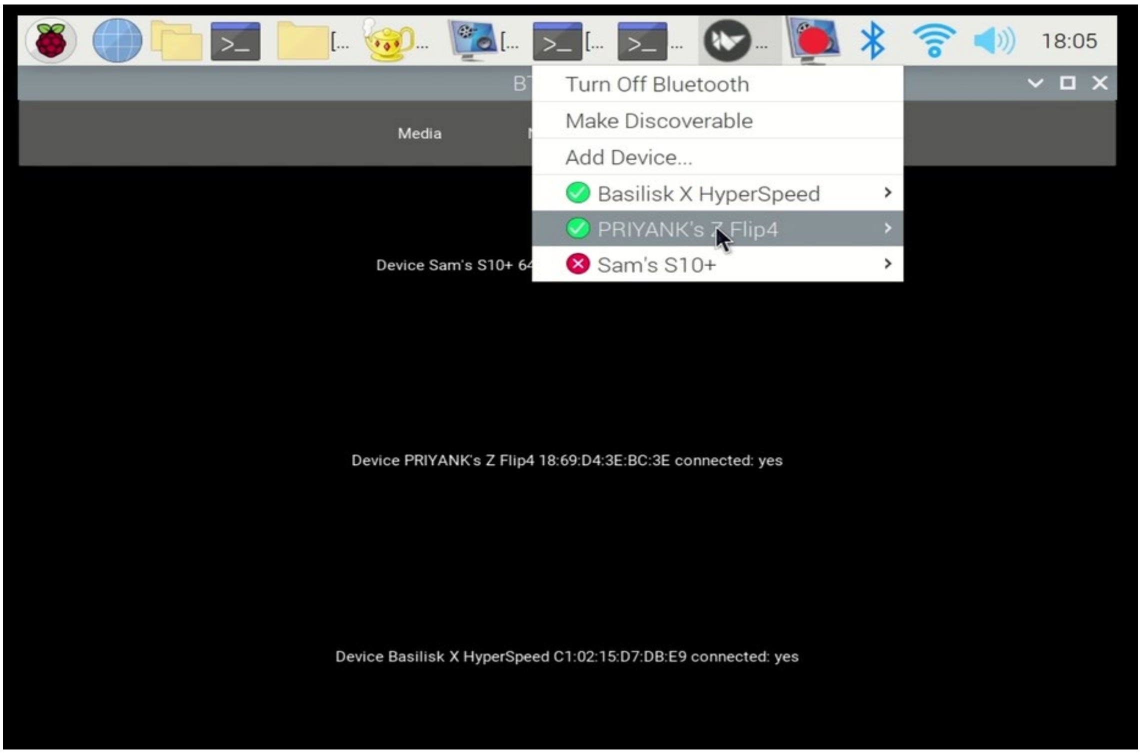


Device Sam's S10+ 64:7B:CE:7B:BA:B3 connected: no

Device PRIYANK's Z Flip4 18:69:D4:3E:BC:3E connected: yes

Device Basilisk X HyperSpeed C1:02:15:D7:DB:E9 connected: yes

Figure 7. Infotainment System Display Showing Current and Previous Paired Devices (“Active” or “Inactive”).

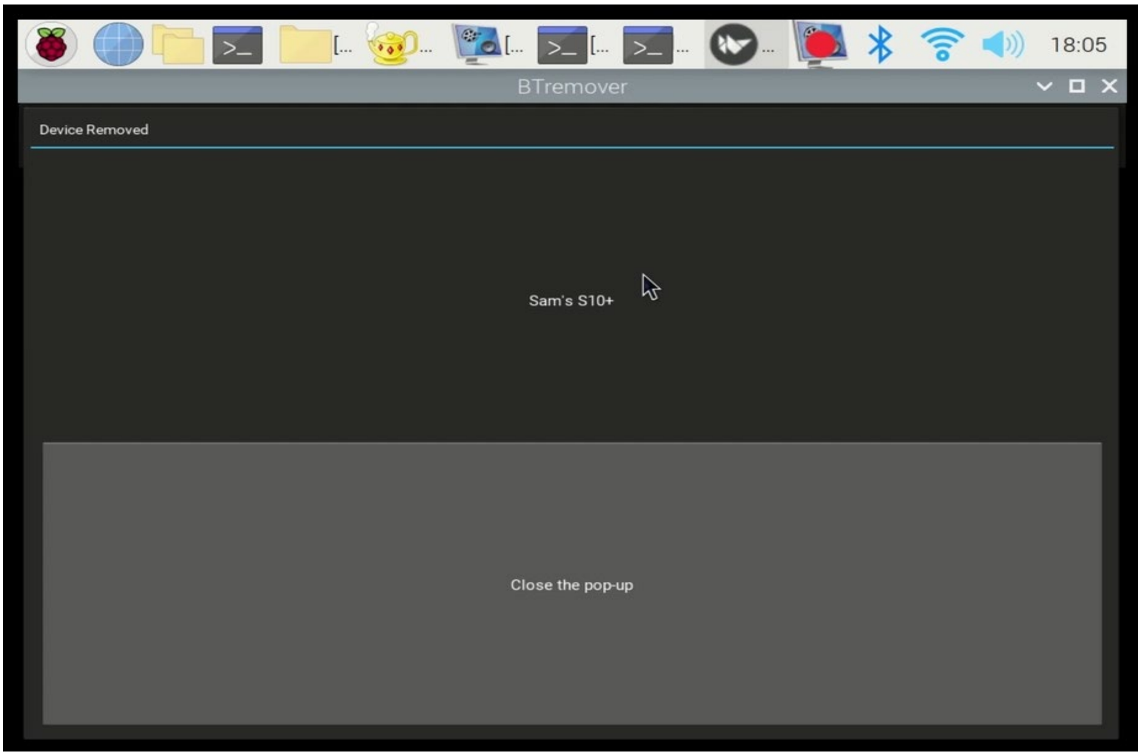


Device Sam's S10+ 64

Device PRIYANK's Z Flip4 18:69:D4:3E:BC:3E connected: yes

Device Basilisk X HyperSpeed C1:02:15:D7:DB:E9 connected: yes

Figure 8. Menu Illustration of Current (Green) and Previous Paired (Red) Devices.



Device Removed

Sam's S10+

Figure 9. VIPR Automatic Removal of "Inactive" Profiles.

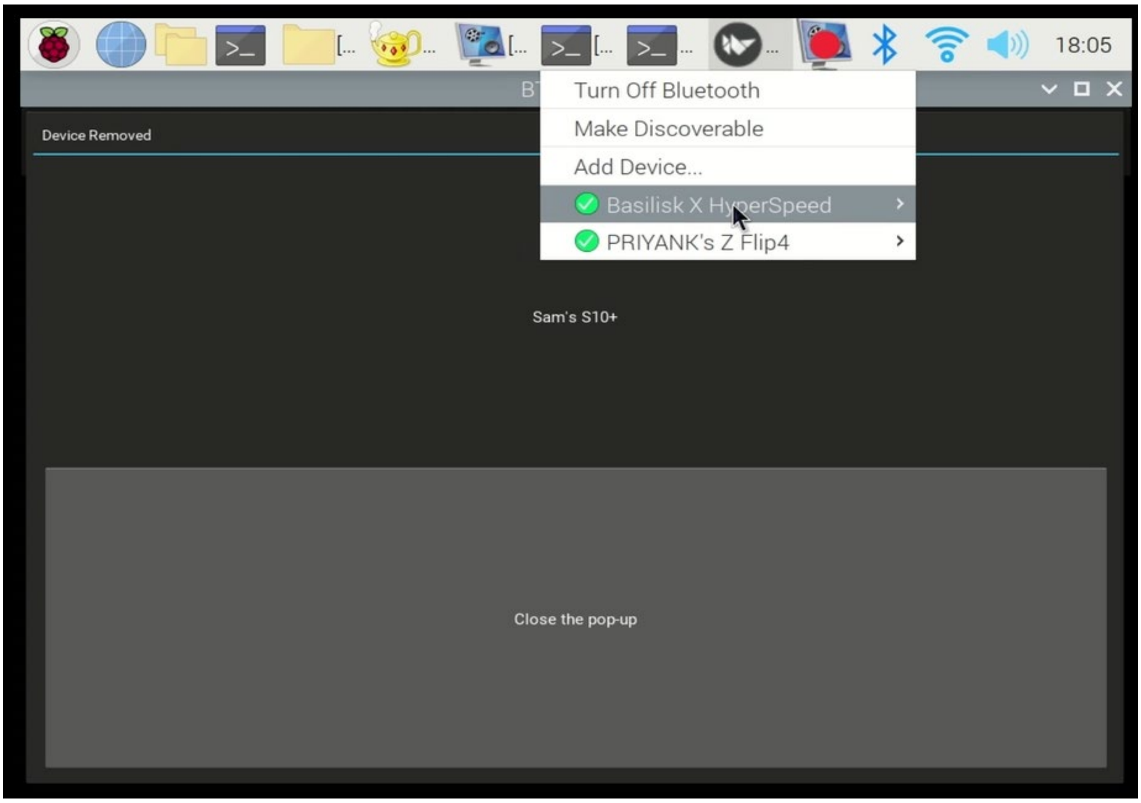


Figure 10. Menu Illustration of "Active" Profiles after VIPR Executes.

7. VIPR Discussion

Each of our experiments successfully met the documented requirements outlined during our planning, analysis, and design phase, which aimed to delete personal information from a rental vehicle automatically. The culmination of these efforts resulted in a successful solution, realized through the development and experimentation of a functional prototype. Utilizing a compact touchscreen interface integrated with a Raspberry Pi unit, we effectively demonstrated the effectiveness of VIPRs in real-world scenarios. This validation reinforces the potential as an advanced solution for enhancing data security and privacy in connected vehicular environments.

This solution comprises lines of code deployed on the Raspberry Pi, effectively emulating a vehicle's Bluetooth stack. VIPR is designed to integrate with existing software technologies such as Ford Sync, Tesla, and others. VIPR leverages the real-time clock embedded in the vehicle's body control module (BCM). As part of the code base used for our experiments, we designed our trials using a recurring time check every 30 seconds to systematically categorize the paired profiles as either **"Active"** or **"Inactive."** In the case of the profiles identified as **"Inactive,"** VIPR seamlessly executes an automatic deletion process on the backend.

8. VIPR Future Work – VIPR 2.0

We at the University of Michigan are excited to announce the latest improvements to our Vehicle Inactive Profile Remover (VIPR) system, version 2.0. This innovative system enhances privacy and security for vehicle users by ensuring that inactive user profiles are removed promptly and efficiently.

With VIPR 1.0, we introduced a solution designed to remove inactive user profiles based on the vehicle's real-time clock. Our team is taking a significant leap forward by integrating advanced biometric technology into VIPR 2.0. This update will employ facial recognition to establish the identity of the driver or renter, eliminating the previous dependency on time-based triggers.

To achieve this, we are harnessing the power of our laboratory set-up, which includes a high-fidelity Raspberry Pi camera, to capture and process biometric data. We plan to develop a robust facial recognition model using industry-standard tools like Visual Studio Code (VS Code). We intend to seamlessly combine this model with the current VIPR system to provide an even more secure and user-friendly experience.

The new system grants vehicle renters immense flexibility. They can authenticate their identity using the vehicle's onboard camera or their personal mobile device's face ID feature. Upon successfully verifying the driver or renter's face, VIPR 2.0 will automatically activate and eradicate all previously stored "Inactive" profiles, thereby maintaining real-time profile hygiene.

Beyond just infotainment units, our vision for VIPR extends into broader transportation applications and the burgeoning Internet of Things (IoT) landscape. Imagine VIPR technology ensuring user privacy across various transport systems such as ride-sharing scooters, bikes, or even public transit systems. Additionally, the same principles could be applied to IoT devices within smart homes and cities, bolstering security and privacy in our digitally connected society.

In conclusion, VIPR 2.0 is paving the way towards creating a more secure, private, and convenient experience for users in the automotive sector and beyond. VIPR is poised to redefine data protection standards in the transportation industry and IoT devices through these enhancements.

9. Conclusions

The proposed framework aims to protect vehicle owners' and renters' personal identifiable information (PII). Our recent research on protecting consumers'/renters' PII has shown that PII is stored on an infotainment system, which is a serious privacy and security concern. Our research concluded that a consumer's/renter's PII is unsafe or protected and is an extensive overall connected vehicle issue. Therefore, to prove our research, we conducted a hands-on study of security and data privacy analysis by renting three vehicles from three rental companies to see if we could view others' PII on the infotainment system. The results of the hands-on study were that we were able to view prior renters' information from each vehicle and then use that to further identify them through the use of the Internet.

To delve deeper and gain a better understanding from renters' perspectives, we conducted a survey to see if renters left their information on the infotainment system, how they would feel about that, or, when finding out that it is their responsibility to delete that information, if renters knew how to perform that manual process. The prevalent process of removing a renter's personal information from an infotainment system is a manual one. Based on research, no automated solution will perform this task for renters.

As a contribution to this space, the development and demonstration of the VIPR present a significant leap forward in addressing the security and privacy concerns associated with connected vehicles. Through extensive research on the core functionality, requirements, and integration with vehicle networks, VIPR displays its capability to seamlessly interface with the existing vehicle infrastructure while effectively managing the paired profiles on the infotainment system.

The effectiveness of our proposed solution—VIPR—is evaluated by performing a set of experiments using a Raspberry Pi with an embedded system. The motivation behind selecting Raspberry Pi is its versatility and availability of an onboard Bluetooth stack. This innovation is a tangible commitment to enhancing data security and privacy within a connected vehicle ecosystem, leaving VIPR as an agnostic solution.

Figures 7 to 11 explicitly capture the essence of VIPR's functionality. From emulating an infotainment system display to categorizing "Active" and "Inactive" profiles/paired devices, our experiments exemplify VIPR's potential to revolutionize how we manage user data within the connected vehicle ecosystem.

The real-time execution of VIPR, highlighted in Figure 10, captures its ability to distinguish and decisively delete "Inactive" profiles or a prior renter's personal information, ensuring that a renter's PII is secure. As illustrated in Figure 11, the infotainment system displays a concise list of the currently "Active" or the current renters paired device after VIPR executes, showing the practicality and efficiency of VIPR's approach.

VIPR's journey from concept to execution not only solidified its technical viability but also hinted at its broader implications in elevating the cybersecurity standards within the automotive industry. The successful experimentations of the solution underscores the potential for VIPR to be a game-changer in the automotive industry, offering a proactive solution to data security and privacy concerns in the connected vehicle domain.

6. Patents

Our commitment to innovation is further encapsulated by a patent filed with the United States Patent Office [16] for the potential incorporation of VIPR into existing connected vehicle software stacks. The patent marks a significant milestone for VIPR, celebrating our role in data security and connected vehicle technologies' advancement. It is a testament to our dedication and an essential step towards ensuring user privacy and security in an increasingly connected world.

Author Contributions: Jason Carlton and Hafiz Malik made substantial contributions to conception, design, and development of VIPR, performed VIPR experiments, composed the manuscript, and documented the final experiment results.

Funding: None.

Data Availability Statement: The supporting data for this manuscript is available upon request directly from the author.

Acknowledgments: N/A.

Conflicts of Interest: All authors declared that there are no conflicts of interest.

References

1. Sanders, R. L. Car Renters Beware Bluetooth Use Can Reveal Your Private Data. USA Today (2018).
2. Capretto, A. These Were The Top-Selling Vehicles In The USA In 2023. CARBUZZ (2024).
3. Romjue, M. Annual U.S. Car Rental Revenue Tops Itself Again at $38.3 Billion. Auto Rental News (ARN) Rental Operations (2023).
4. Jones, P. Rental Car Demographic: 59 User Facts & Numbers [2023]. Motor and Wheels (2023).
5. Jones, P. How Often Are Rental Cars Replaced? (Checked & Explained). Motor and Wheels (2022).
6. Carlton, J. Security and Privacy Analysis on Rental Vehicles on Consumers Personal Identifiable Information (PII). (2022).
7. Carlton, J. A Data Privacy Survey on Personal Identifiable Information (PII) on Rental Vehicle Infotainment Systems. (2023).
8. Staff, A. R. New app claims to wipe personal info left in infotainment system. Auto Remarketing (2018).
9. Commission, F. T. The Connected Cars Workshop: The Federal Trade Commission Staff Perspective. https://www.ftc.gov/system/files/documents/reports/connected-cars-workshop-federal-trade-commission-staff-perspective/staff_perspective_connected_cars_0.pdf (2018).
10. (GAO), G. A. VEHICLE DATA PRIVACY Industry and Federal Efforts Under Way, but NHTSA Needs to Define Its Role. https://www.gao.gov/assets/gao-17-656.pdf (2017).
11. Force, N. J. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. National Institute of Standards and Technologies (NIST) (United Department of Commerce, United States, 2018).
12. International, P. Connected Cars: What Happens to Our Data on Rental Cars? Privacy International (2017).
13. Carlton, J. Rental Car Mobile/Data Synchronization. https://forms.office.com/Pages/DesignPageV2.aspx?origin=NeoPortalPage&subpage=design&id=DQSIkWdsW0yxEjajBLZtrQAAAAAAAAAAAAN__tcIcdVUNzhYT1VHNUtRQ0w3N0xSV0ZRMFdGTVFUQS4u&analysis=false (2023).
14. Lacroix, J. Vehicular Infotainment Forensics: Collecting Data and Putting It into Perspective. https://ontariotechu.scholaris.ca/items/40ba2fc3-f7ff-4c66-8a04-e388a11cf579 (2017)
15. Carlton, J., Malik, H., Shah, P. 2023. Vehicle 'Inactive' Profile Remover, United States of America Patent No. 84555470

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.