Journal of
Sensor and Actuator Networks

MDPI

Article

Safeguarding Personal Identifiable Information (PII) after Smartphone Pairing with a 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 (CAVs) has significantly enhanced driving convenience, but it has also raised serious privacy concerns, particularly regarding the personal identifiable information (PII) stored on infotainment systems. Recent advances in connected and autonomous vehicle control, such as multi-agent system (MAS)-based hierarchical architectures and privacy-preserving strategies for mixed-autonomy platoon control, underscore the increasing complexity of privacy management within these environments. Rental cars with infotainment systems pose substantial challenges, as renters often fail to delete their data, leaving it accessible to subsequent renters. This study investigates the risks associated with PII in connected vehicles and emphasizes the necessity of automated solutions to ensure data privacy. We introduce the Vehicle Inactive Profile Remover (VIPR), an innovative automated solution designed to identify and delete PII left on infotainment systems. The efficacy of VIPR is evaluated through surveys, hands-on experiments with rental vehicles, and a controlled laboratory environment. VIPR achieved a 99.5% success rate in removing user profiles, with an average deletion time of 4.8 s or less, demonstrating its effectiveness in mitigating privacy risks. This solution highlights VIPR as a critical tool for enhancing privacy in connected vehicle environments, promoting a safer, more responsible use of connected vehicle technology in society.

Keywords: connected vehicles; data privacy; data security; infotainment systems; personal identifiable information; automated solution; VIPR; cybersecurity; rental vehicles

check for updates

Citation: Carlton, J.; Malik, H. Safeguarding Personal Identifiable Information (PII) after Smartphone Pairing with a Connected Vehicle. *J. Sens. Actuator Netw.* **2024**, *13*, 63. https://doi.org/10.3390/jsan13050063

Academic Editors: Jordi Mongay Batalla, Pascal Lorenz and Ioannis Chatzigiannakis

Received: 29 August 2024
Revised: 3 October 2024
Accepted: 4 October 2024
Published: 6 October 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

As the Internet of Things (IoT) becomes increasingly integrated into modern life, maintaining the security of personal information stored in devices ranging from CAVs to general smart gadgets has become a challenge. The proliferation of these IoT and intelligent transportation systems has ushered in a new era of convenience and efficiency yet simultaneously poses a formidable challenge in protecting the troves of PII they collect, store, and process. For instance, safeguarding the personal information stored in infotainment systems after pairing smartphones remains a significant challenge for CAVs [1].

The development of CAVs has led to significant advancements in the areas of cooperative driving and autonomy. A study has demonstrated promising outcomes in enabling the cooperation of multiple CAVs to improve traffic efficiency, safety, and energy consumption. For instance, MAS based hierarchical architecture has been proposed for the cooperative control of CAVs, highlighting the potential of advanced coordination to achieve optimal vehicle behavior. This MAS architecture supports communication and decision-making among multiple autonomous agents (vehicles), facilitating coordinated maneuvers such as platooning and lane merging [2].

However, while cooperative control frameworks such as MAS-based architectures improve traffic efficiency, they also introduce critical data privacy challenges. The growing amount of data exchange between vehicles requires strong privacy-preserving strategies to protect sensitive information. A recent study proposed a parameter privacy-preserving

strategy for mixed-autonomy platoon control, which ensures that vehicle control parameters are kept confidential during cooperative maneuvers. This approach effectively addresses privacy risks in mixed traffic environments, emphasizing the need for privacy measures in cooperative CAV systems [3].

The interconnected nature of CAVs and the potential for privacy risks highlight the importance of ensuring adequate data security, particularly in scenarios where personal data, such as contact information and location history, can be left on shared vehicle systems. This is especially critical in the vehicle rental market, where rental cars equipped with infotainment systems pose substantial challenges. Renters often fail to delete their data after use, leaving it accessible to subsequent renters. Without an automated solution, these privacy risks are likely to persist.

1.1. PII Vulnerabilities in the Rental Market

Industry forecasts in the rental market indicates a robust growth in connected vehicles, with approximately 15.5 million IoT-equipped vehicles expected to enter the US market in 2023 alone [4]. As the number of connected vehicles increases, so too does the risk of exposure of personal data if adequate privacy measures are not put in place.

The vehicle rental market is extremely susceptible to PII leakage due to a lack of regulations and protocols for protecting renters' data after the vehicle is returned. As depicted in Table 1, the US rental vehicle market expanded from 2,111,921 vehicles in 2022 to 2,263,900 vehicles in 2023, representing 15% of the population [5]. According to Peter Jones of Motor and Wheels, the average rental period is in the range of two to three days [6], and companies typically retain their fleet for two to four years [7]. Over the course of time rental vehicles undergo multiple short-term rental cycles throughout their lifecycle, raising the risk that PII will be stored in the infotainment systems and accessed by unauthorized individuals.

Table 1. The table shows 2022 US rental vehicles in service.

2022 US Car Rental Market by Fleet, Locations, and Revenue				
Company	**US Cars in Service (Avg.) 2022**	**Number of US Locations**	**2022 US Revenue Est. (Millions)**	**2021 US Revenue (Millions)**
Enterprise Holdings (St. Louis, MO, USA, includes Alamo Rent-A-Car, Enterprise Rent-A-Car, National Car Rental)	1,200,000	5500	19,915	15,664
Avis Budget Group (Parsippany-Troy Hills, NJ, USA, includes Payless, not Zipcar)	425,000	3000	8430	6045
Hertz (Estero, FL, USA, includes Dollar and Thrifty)	365,000	3900	5700	5600
Sixt (Pullach, Germany)	29,000	98	970	650
Fox Europcar (Los Angeles, CA, USA)	18,571	27	391	330
ACE Rent-A-Car (Indianapolis, IN, USA)	12,000	75	120	100
NP Auto Group (Laurel, MD, USA, Priceless and NextCar)	7350	101	62	50
Green Motion U-Save Group	8500	84	40	33
Rent-A-Wreck of America (Laurel, MD, USA)	1500	60	15	16
Independents	45,000	3800	450	425
Totals	2,111,921	16,645	36,093	28,913

Rental vehicles are also equipped with various communication technologies such as Wi-Fi, LTE/5G, Dedicated Short Range Communications (DSRCs), and Vehicle-to-

Everything (V2X) communications (Figure 1). Traditional in-vehicular networks (VANETs), including Controller Area Network (CAN), Media-Oriented Systems Transport (MOST), Local Interconnected Network (LIN), and FlexRay, are intertwined with advanced sensor fusion systems that enable autonomous driving, traffic management, and predictive maintenance [8] (Figure 2). These interconnected systems distribute PII across multiple nodes, increasing the potential for privacy violations, especially when pairing a mobile device or sharing locations [9] to an infotainment system.

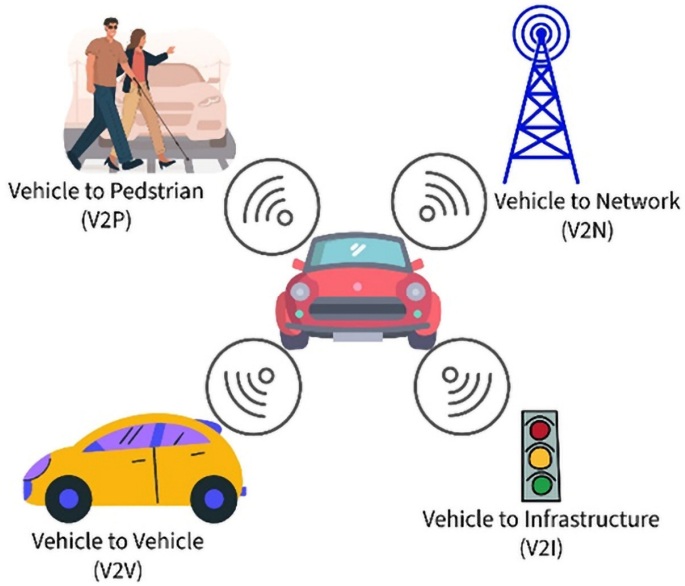


Figure 1. Illustration of the Vehicle-to-Everything (V2X) communications model.

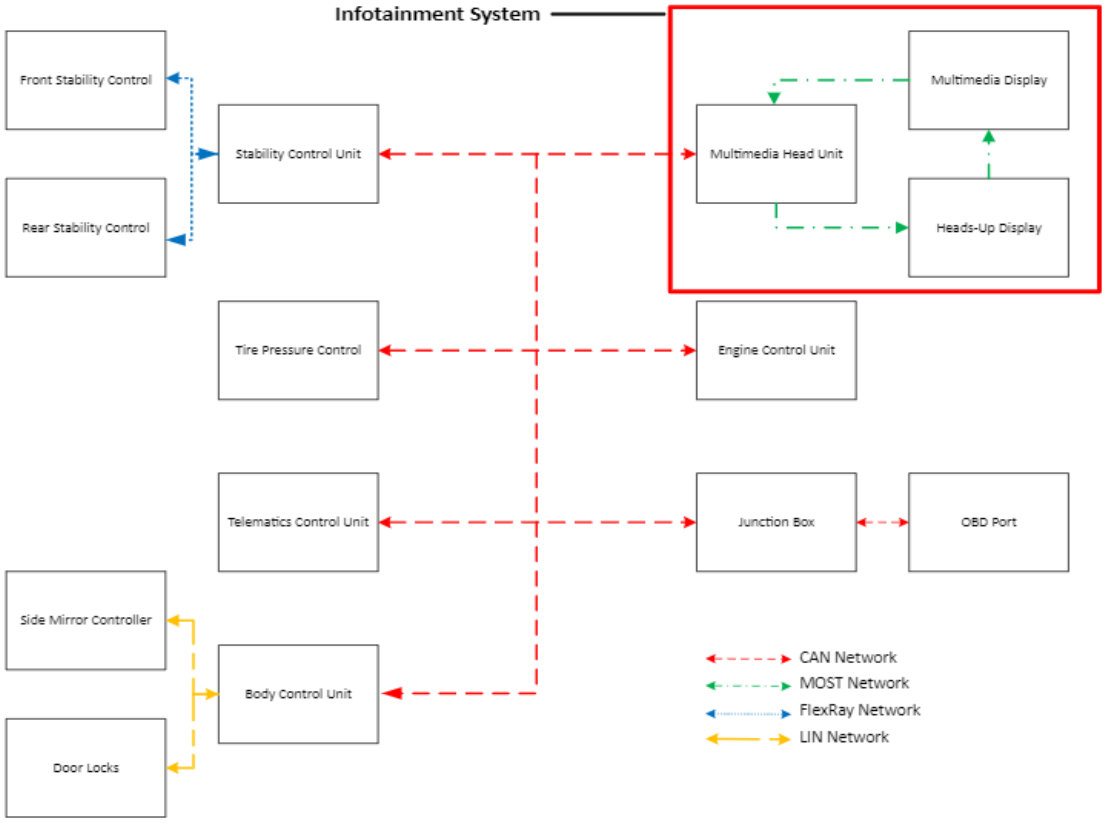


Figure 2. Illustration of modern in-vehicle network architecture.

1.2. Challenges in PII Removal from Rental Vehicles

The proliferation of CAV technologies has led to significant challenges in managing PII in the rental vehicle market. To gain a better understanding of how large the issue was, we performed a hands-on study [10] that involved renting three different rental vehicles from three different rental providers (Enterprise, Hertz, and Turo), which revealed that each vehicle retained sensitive PII from the previous renters, such as contact lists and GPS navigation data. This retention of sensitive PII occurred because renters did not manually delete their data prior to its return, resulting in it being accessible to subsequent users [8,9]. This oversight poses serious privacy risks, particularly given that rental cars are frequently used by different individuals over their lifecycle. The Federal Trade Commission (FTC) noted that a rental car might keep personal information long after it has been returned, emphasizing the critical need for a solution that can secure renters' data [11]. For more details on our study, please refer to Section 3.

To gain a deeper understanding of the awareness and behaviors of rental vehicle users regarding PII retention, we conducted a survey [12] that targeted rental customers. Out of 120 respondents, 83.3% indicated that they highly valued their personal information; however, most were unaware of the need to delete their PII manually after using the vehicle. This lack of awareness further exacerbates the risks associated with PII leakage. All of the participants in the survey expressed support for an automated solution that could handle PII deletion on their behalf, highlighting the desire for a more seamless and secure approach. Detailed survey findings are presented in Section 4.

These findings highlight the necessity for a robust solution to protect PII in rental vehicles. The Vehicle Inactive Profile Remover (VIPR) is an automated technical solution designed to address these challenges. Therefore, this paper focuses on the design and implementation of the Vehicle Inactive Profile Remover (VIPR), an automated technical solution for PII removal. VIPR distinguishes between "Active" and "Inactive" profiles within a vehicle's Bluetooth stack, expunging PII from inactive profiles at defined intervals to ensure user data are securely deleted (Figure 3). For further details, please see Section 6.

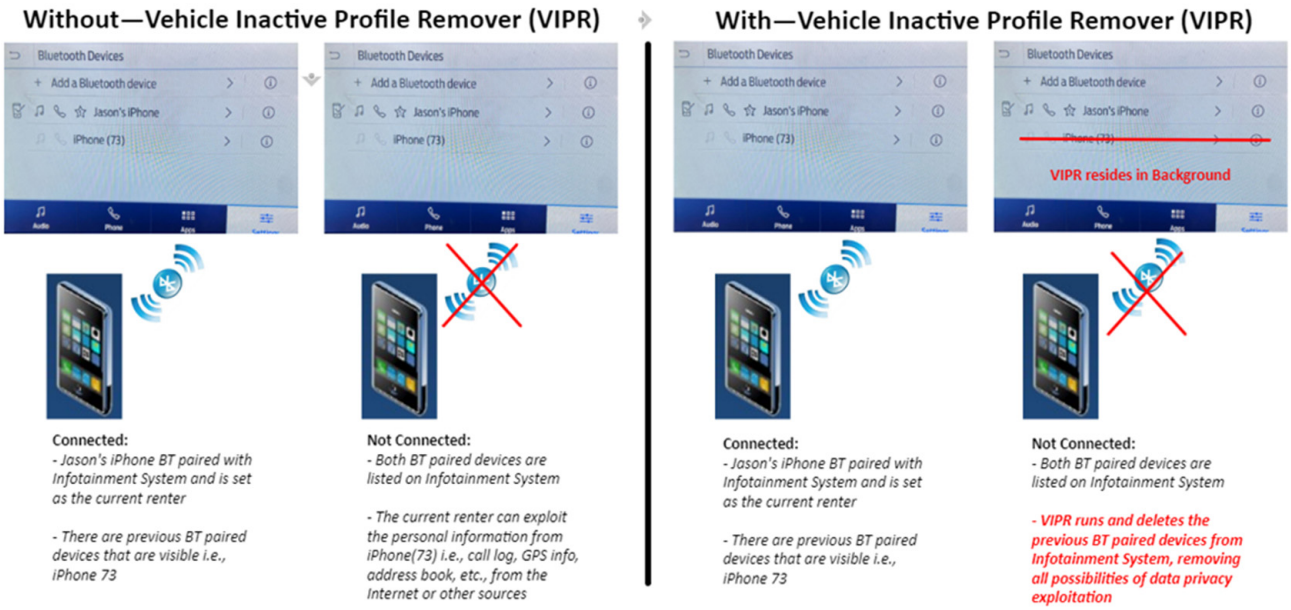


Figure 3. High-level illustration PII leakage through Bluetooth pairing and removing user profiles using VIPR.

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

1. Comprehensive Review of PII Threats: This study systematically explores privacy risks specific to the IoT and CAV 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, such as the European Union GDPR [12] and the California Consumer Privacy Act (CCPA) [13].
4. Development of a Universal Solution: Introducing Vehicle Inactive Profile Remover, a cross-sectoral technology designed to automate the erasure of PII from an Infotainment System including all types of connected vehicles, creating a safer digital environment.
5. Experimental Validation: The experimental results demonstrate the effectiveness of the universal 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 use of biometrics for driver authentication to enhance a safer digital environment for CAVs.
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 dialog on privacy and trust in an automated age [14].

1.3. Summary

The integration of CAVs into the transportation landscape has brought significant advancements in terms of convenience and driving experience. However, this connectivity also introduces critical privacy concerns, particularly related to the removal of PII on vehicle infotainment systems. Rental vehicles, in particular, are at a heightened risk for PII leakage due to frequent turnover among renters and a lack of standardized data protection protocols. Our study reveals that PII, such as contact lists and navigation data, is often left behind by renters, posing serious privacy risks when accessed by subsequent renters.

To address this privacy risk, we developed a solution called the Vehicle Inactive Profile Remover (VIPR). VIPR is an automated solution designed to delete PII from infotainment systems. VIRP ensures data privacy and trust of renters by preventing unauthorized access to PII in rental vehicles.

2. Related Work

The rapid integration of connected vehicle technology has significantly complicated the task of protecting consumers' personal information within rental vehicle 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 of automated methodologies to reduce this risk, we scrutinized a variety of approaches. A particular highlight among these is Privacy4Cars [15], 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 [16]. 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 guarantee of greater interoperability and information exchange among OEMs, the refinement of the 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 [17], requesting input from 16 OEMs about their data-handling practices related to connected vehicles. Of the respondents, only 13 OEMs admitted to 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) [18]. 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 desirable against the backdrop of software-centric modern vehicles, which introduce broader attack vectors and thus greater opportunities for malicious entities to acquire personal data.

A pre-emptive 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 any such 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 are 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 "Security and Privacy Analysis on Rental Vehicles: Assessing Potential Vulnerabilities to Consumers' Personal Identifiable Information (PII)" [10], an investigative study that 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.

This study involved the rental of three distinct vehicles from Hertz, Enterprise, and Turo, scrutinizing each for traces of PII left by previous renters [19]. 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 revealed 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 aligned with findings from a report by USA Today, which expressed similar concerns about the privacy policies of major

rental companies like Enterprise, Hertz, Zipcar, and Europcar [1]. Every rented vehicle from these companies retained the personal data of its previous users.

Our study strengthens the argument that previous renters' PII must 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. According to Danny Palmer a senior writer at ZDNET, "Most of the companies involved say the rules on deleting user information are in the terms and conditions for the car hire, but according to Privacy International, these aren't made clear to users—and their passengers" [20]. The study advocates for industry-wide changes to ensure that consumer data are consistently and effectively protected, including reforming privacy policy disclosures and introducing mandatory PII removal notifications for customers before vehicle return. These recommendations aim to reduce 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 leaving their personal information in 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"—and potentially accesses a navigation history that reveals the travel patterns of past users [21].

This survey was disseminated to 600 individuals via several social media avenues, including community groups on Facebook and professional networks such as 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. According to Dasom Lee and David Hess stated, "Nevertheless, survey respondents located in the U.S. who show a higher level of privacy concern about CAVs or about using Internet or Internet-enabled technologies are also less likely to want to use CAVs" [22]. It is notable that only 67.5% of the participants showed varying degrees of tolerance on a scale from 1 to 5 on the question about the tradeoff between comfort level and the risk of their information being shared with subsequent renters [23,24].

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 [25]. 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 did not know or were unsure about 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 need 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 can transform the car rental experience, ensuring personal data are cleared without requiring specific action from the user, thereby preventing potential privacy breaches and establishing a new standard for protecting personal information within the rental car industry.

5. Proposed Framework to Safeguard PII in Rental Vehicles

To address the risks associated with PII in rental vehicles, we developed, the Vehicle Inactive Profile Remover (VIPR)—an advanced software-based solution designed to automatically delete renters PII from the infotainment systems. VIPR operates by marking all profiles as active or inactive based on their paring status, and deleting the inactive profiles at defined intervals, ensuring that any residual data from previous renters is systematically removed. VIPR will address the following three rental scenarios 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 [26].
2. Subsequent Rentals: Highlights rental organizations' responsibility to delete renters' PII before a subsequent rental.
3. Ride-sharing: 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

The development of VIPR was designed for effectiveness and seamless integration into existing vehicle technology ecosystems by the following ten key requirements as shown in Table 2.

Table 2. Ten VIPR foundational requirements.

Framework Requirements	
Requirement No.	**Requirement 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 delete profiles paired with Bluetooth
5	Should be able to delete profiles paired with Apple Car Play and/or Android Auto
6	Must integrate within the 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 and Architecture

To ensure the successful implementation of VIPR, our approach included a detailed analysis of the existing in-vehicular network (IVN) architecture and the integration of VIPR within these vehicle systems. The analysis aimed to ensure that VIPR could seamlessly function alongside current vehicle networks such as the Controller Area Network (CAN), Media-Oriented Systems Transport (MOST), and Local Interconnected Network (LIN) systems, which are integral to various subsystems like the stability control unit and engine control units. This integration was designed to meet the essential framework requirements

detailed in Table 2, ensuring compatibility and efficient operation within the existing vehicle infrastructure.

5.3. VIPR Architecture and State Diagrams for Data Deletion Framework

To address the challenges of securing PII in rental and ride-sharing scenarios, we designed VIPR's architecture by translating our framework requirements into state diagrams. These state diagrams visually clarify the strategy and operational flow of the VIPR system, helping to simplify the complex interactions involved in managing and removing PII. Below, we present two core use cases: rental vehicle depot return and ride-sharing.

5.3.1. Rental Vehicle Depot Return and Subsequent Rentals

For the rental depot and subsequent rental process, we outlined a six-step sequence to ensure that inactive renter profiles are automatically detected and removed. The proposed process, illustrated in Figure 4, is detailed as follows:

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, it is prepared by the rental organization for a subsequent renter.
3. Existing "Profiles": The new renter pairs their mobile phone to the vehicle and finds 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 s.
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.

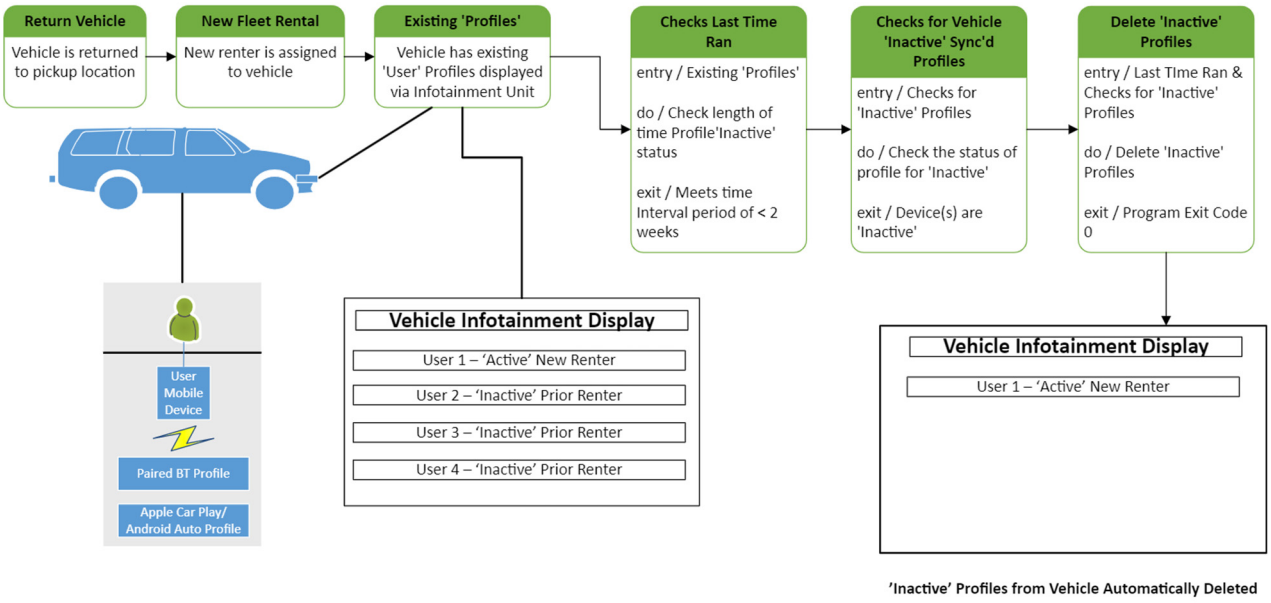


Figure 4. VIPR state diagram for rental vehicle depot return and subsequent rentals.

5.3.2. Ride-Sharing Scenario

For the ride-sharing scenario, we developed a three-step sequence to ensure the secure handling of PII, as shown in Figure 5. This process includes an additional feature where a renter can manually delete their personal data before exiting the vehicle. The steps are as follows.

1. Pick Up Vehicle: The rental vehicle is picked up from a remote location, such as a city street.

2. Existing Pre-Defined Locations: The infotainment system is checked for inactive profiles, i.e., previous renters' location histories and personal information.
3. Prompt on Infotainment Display: Once the rental is completed, the vehicle is returned to the same location. When turned off, a prompt will appear on the infotainment system, allowing the renter to delete their personal information manually. If the renter opts out, the program will still execute deletion at the established pre-defined time.

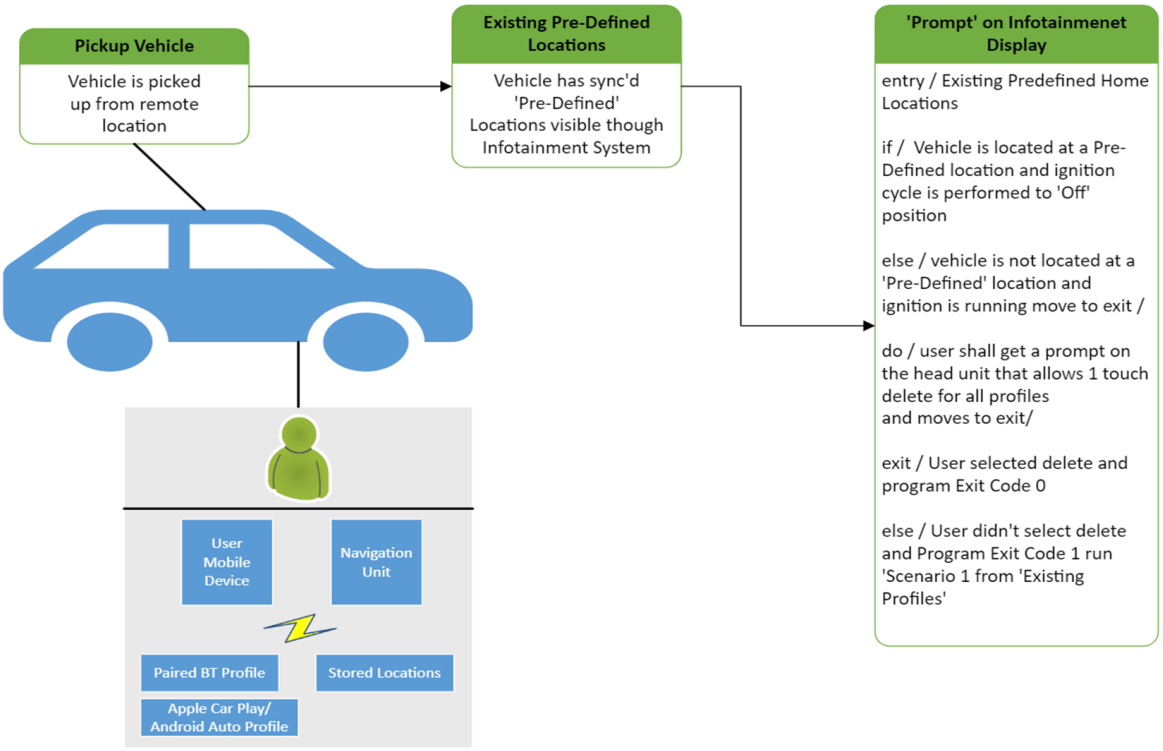


Figure 5. VIPR state diagram for ride-sharing.

These state diagrams and processes are integral to VIPR's ability to seamlessly handle data deletion, automate profile management, and address PII security challenges in rental and ride-sharing scenarios. By integrating VIPR into existing vehicle architectures, we ensure that renters' privacy is maintained without manual intervention, providing a robust solution to the ongoing challenge of protecting personal data in connected vehicles.

5.4. VIPR Mathmatical Model

To effectively demonstrate the functionality and performance of the Vehicle Inactive Profile Remover (VIPR) system, we developed a detailed mathematical model. This model formalizes the key processes involved in identifying, deleting, and verifying the removal of PII from a rental vehicle's infotainment system. By modeling the data deletion process, we can quantify the effectiveness and efficiency of VIPR, simulate various operational scenarios, and establish the theoretical underpinnings of our automated solution. The following outlines the critical components of the model, including data storage, defined time mechanisms, deletion algorithms, and verification processes.

1. Data Storage: This is where data being stored, data being used by the current renter, and data which must be deleted are defined as follows:
    - D_t: Total data stored in the infotainment system at time t.
    - D_{renter}: Data belonging to a specific renter that must be deleted.
    - D_i: Infotainment system (not related to the renter) that must be retained.
    - At any time t, the total data can be expressed as follows:
        - $D_t = D_{renter} + D_i$

2. Defined Timed Mechanism: t is defined as the time that the deletion process is executed.
   - $t = T_{interval}$
3. Deletion Algorithm: The system performs the deletion of D_{renter} by applying the deletion function δ.
   - $D_{renter}(t) = D_{renter}(T_{interval}) \times e^{-\lambda t}$
   - λ is the rate of data deletion and $D_{renter}(t)$ approaches zero as time t increases, indicating the completion of the deletion process.
4. Verification Process: The system verifies that renter data have been removed from the system, where $V = 1$ means the deletion was successful OR $V = 0$, meaning that the deletion failed or is incomplete.
   - $V = \{1$, if $D_{renter} = 0$ after deletion OR $V = \{0$, if $D_{renter} > 0$ after deletion
5. Probability of Success: Based on the deletion algorithm and the identification accuracy of user data, where $P_{success}$ is the probability of successful data deletion.
   - $P_{success} = P(D_{renter} = 0 \mid t > T_{internval}$

Our mathematical model outlined above provides a rigorous framework for understanding the operational dynamics of the Vehicle Inactive Profile Remover (VIPR) system. Incorporating data identification, deletion algorithms, and verification mechanisms, the model ensures that the system efficiently removes personal data while minimizing risks of residual information. This formal approach not only validates the theoretical viability of VIPR but also sets the foundation for practical implementation, optimizing privacy protection for renters in CAVs. The model serves as the foundation for both theoretical validation and practical implementation of VIPR in real-world applications, as clearly displayed in Section 6.

6. VIPR Experiments and Results

To validate VIPR, we established a controlled laboratory environment using a Raspberry Pi with Wi-Fi and Bluetooth capabilities, along with a 7-inch touchscreen display to emulate the interface of a vehicle infotainment system. We developed Python code that implemented the key requirements of the VIPR system—checking, validating, and deleting inactive profiles. This section outlines the series of experiments that validated our technical solution.

6.1. Experiment 1: Vehicle Infotainment System Replication

In this experiment, we accurately replicated the interface of an actual connected vehicle infotainment system using the 7-inch touchscreen display, as shown in Figure 6. This replication allowed us to create a realistic test environment where all key functions of the infotainment system could be evaluated, providing a reliable basis for further experiments.

6.2. Experiment 2: Collecting Paired Devices and Their Status

In this experiment, we demonstrated how the VIPR solution collects data on paired devices and their respective states. The infotainment system displayed a list of paired device profiles on the 7-inch touchscreen, distinguishing between active and inactive connections. By clicking on the paired button, the system showed the real-time status of paired devices—Yes for active connections (current renters' device) and No for inactive connections (prior renters' device)—as shown in Figure 7. This functionality forms the foundation for the identification of inactive profiles, which are subsequently targeted for deletion.

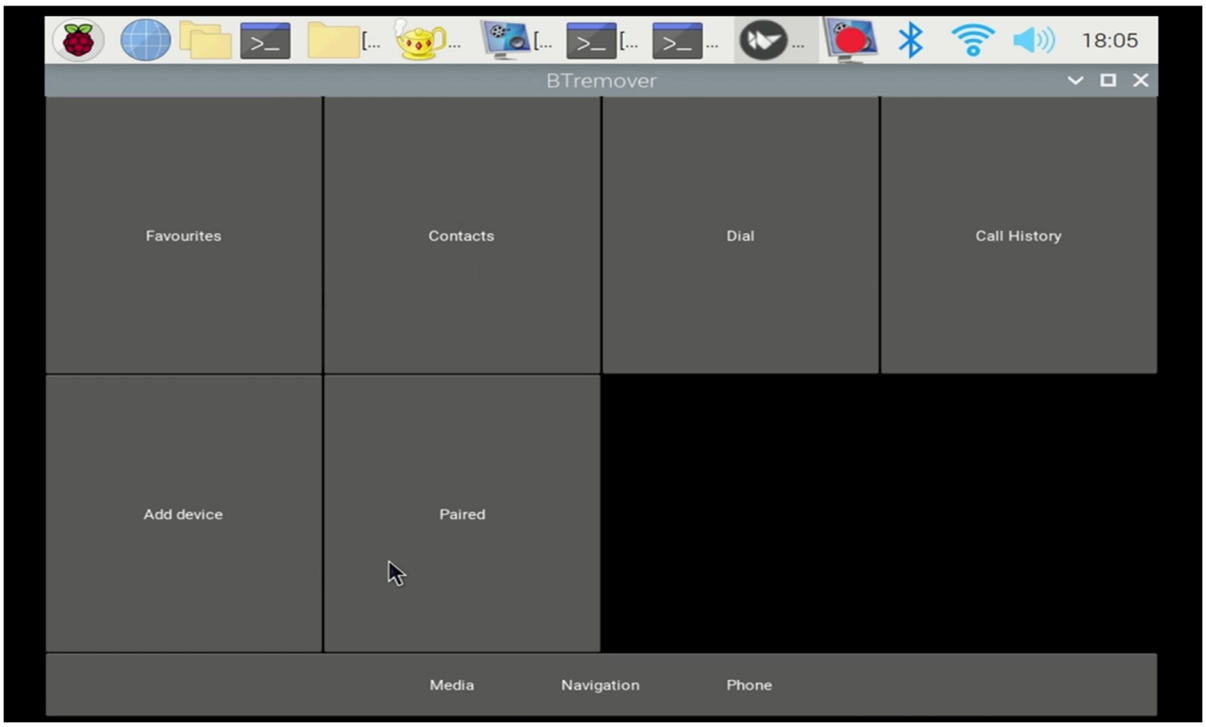


Figure 6. Replicated vehicle infotainment system.

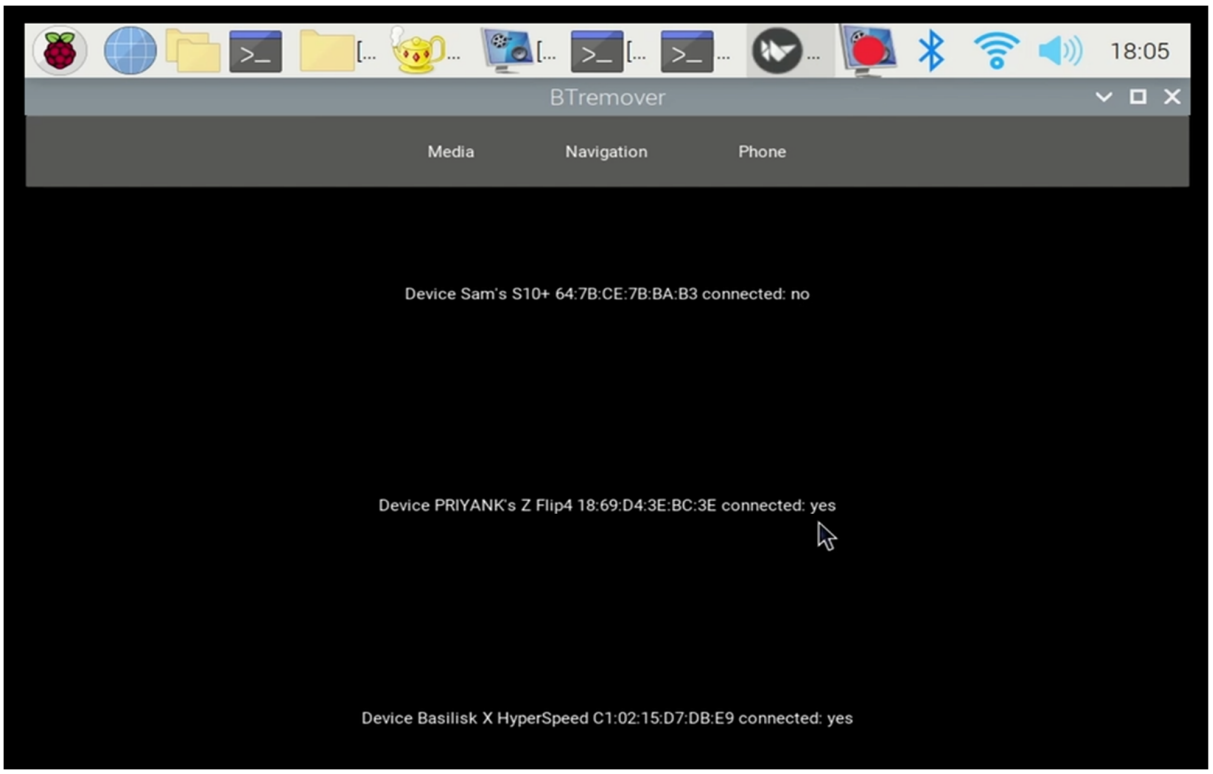


Figure 7. Infotainment system display showing current and previous paired devices (active or inactive).

6.3. Experiment 3: Viewing Current and Previous Paired Devices

This experiment involved testing the user interface to view the current and previously paired devices in the infotainment system. A renter could interact with the system by selecting the Bluetooth menu item, which presents a list of all connected devices. In Figure 8, green status buttons represent active paired devices (indicating current renters), whereas red status buttons represent inactive paired devices that are queued for deletion. This visual representation helps renters quickly identify their devices and ensure any prior renter profiles are not retained.

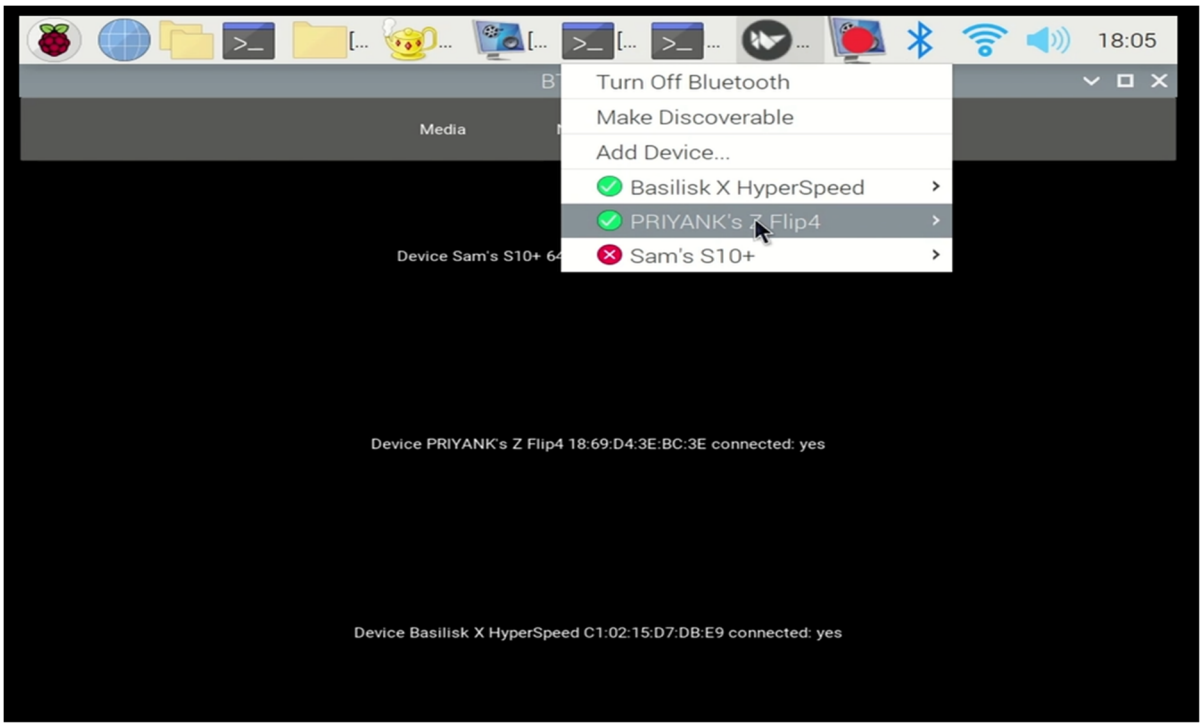


Figure 8. Menu illustration of current (green) and previous (red) paired devices.

6.4. Experiment 4: The VIPR Automatically Removing Inactive Profiles

To validate the automated deletion process, we conducted an experiment where the VIPR removed the inactive profile labeled as "Sam's S10+". As shown in Figure 9, the success of this experiment was indicated by the absence of the inactive profile in the updated list of paired devices. This result validated the VIPR's capability to efficiently and automatically delete inactive profiles without requiring manual intervention. The incorporation of an adaptive deletion rate (as suggested) ensured that the deletion process was executed efficiently, depending on system load and operational conditions.

6.5. Experiment 5: Checking Active Profiles after Inactive Profiles Are Deleted

In this final experiment, we verified that all inactive profiles were successfully deleted, leaving only the active profiles in the infotainment system. Figure 10 shows the list of active profiles remaining after executing the deletion of inactive profiles in Experiment 4. This scenario simulated a current renter who paired their device with the rental vehicle. An additional verification step was introduced at this stage to ensure that the deletion was thorough and complete. This redundancy was implemented to address any potential issues with residual data, thereby providing a more secure system for future renters.

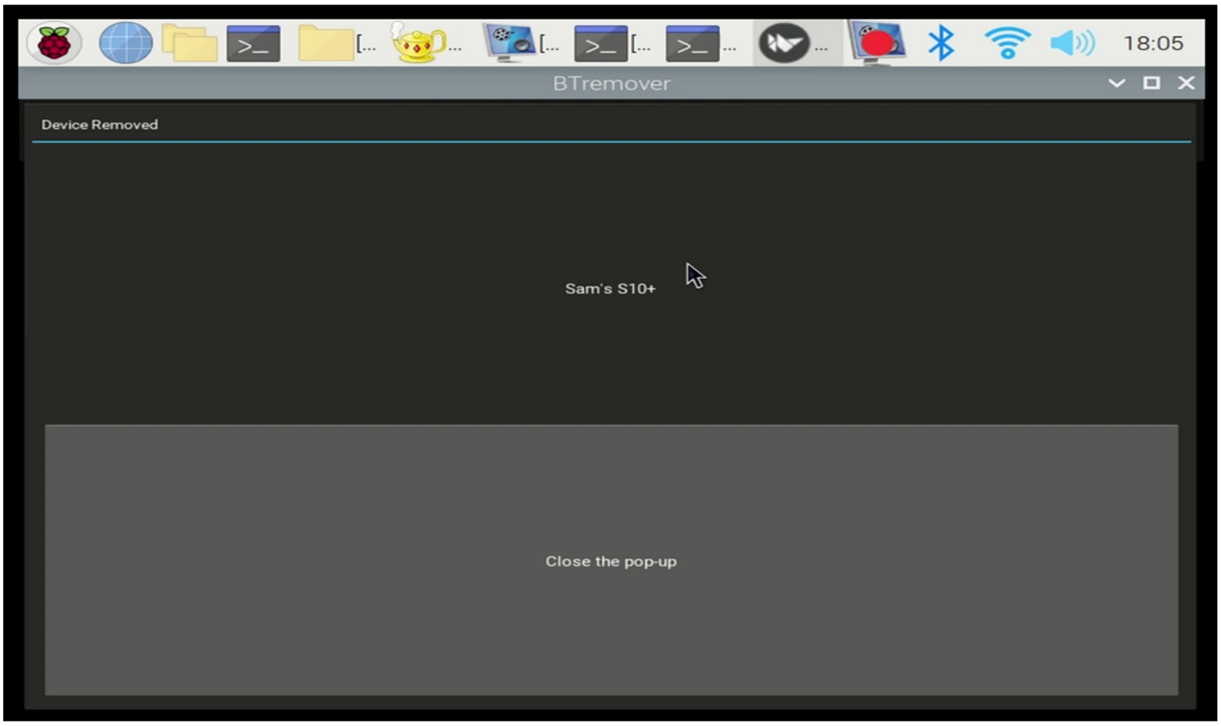


Figure 9. VIPR automatic removal of inactive profiles.

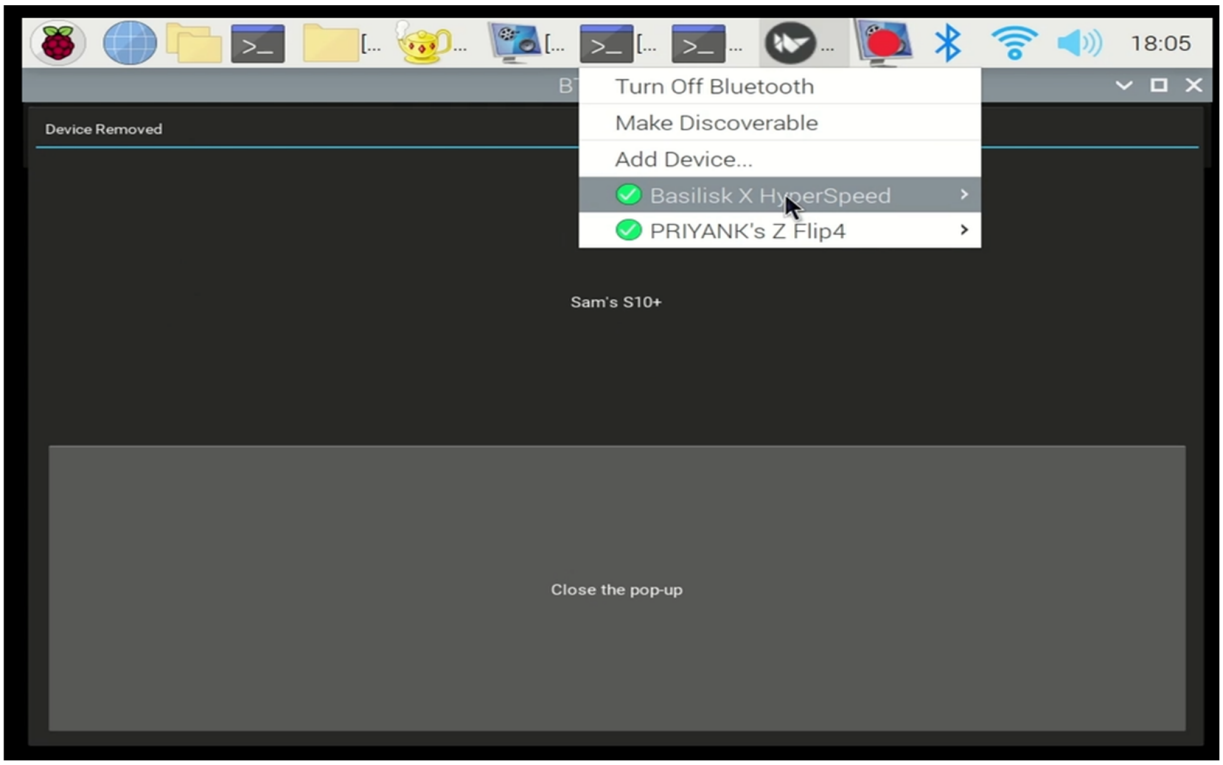


Figure 10. Menu illustration of active profiles after the VIPR executes.

In summary, the experimental evaluation of the Vehicle Inactive Profile Remover (VIPR) system focused on several key performance metrics, as outlined in the mathematical model. These metrics included the time taken to delete PII, the success rate of data deletion, system efficiency, and error rates. The experiments were conducted using a simulated rental vehicle environment, replicating real-world conditions, where renters often leave personal

data in infotainment systems. As predicted by the model, VIPR successfully deleted all user profiles with an average deletion time of 4.8 s or less and achieved a success rate of 99.5% when utilizing the existing vehicle technology ecosystem.

7. VIPR Discussion

The successful experiments with VIPR highlight its potential to fill the existing gap in the protection of PII in rental vehicles. Manual data deletion processes put an undue burden on renters and result in significant privacy vulnerabilities. VIPR automates this process, removing human error and reducing risks associated with manual intervention.

7.1. Real-World Implications

In real-world scenarios, the VIPR system would seamlessly operate in the background of connected vehicles, ensuring renters' privacy without the need for them to manually delete their personal data. By integrating into the vehicle's existing network, VIPR works in tandem with OEM software technologies like Ford Sync or Tesla's software, ensuring broader compatibility across different manufacturers.

7.2. Advantages over Existing Solutions

Unlike existing manual deletion guides, VIPR provides a true automated solution, capable of consistently identifying and removing sensitive data without renter input. The system uses a time-based mechanism and verification process to ensure thorough data deletion, minimizing the risk of PII leakage. VIPR's efficiency in achieving a 99.5% success rate for data deletion and its ability to operate seamlessly demonstrates a significant advancement over available alternatives like Privacy4Cars, which rely on manual processes.

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. Building on the success of VIPR 1.0, we propose an enhanced version—VIPR 2.0—that integrates biometric technology for even greater security. The new system will use facial recognition to establish the identity of the driver or renter, eliminating the need for a time-based trigger.

VIPR 2.0 will be tested using a Raspberry Pi camera and facial recognition model, developed with Visual Studio Code (VS Code). By verifying the renters' identity using onboard cameras or personal mobile device face ID features, VIPR 2.0 will automatically delete inactive profiles, ensuring a secure environment for the next renter. Our team researched hand and speech technology for VIPR 2.0 but is limited to slow performance and false/positives [27].

Beyond rental vehicles, VIPR technology could also be applied across broader transportation modes and the expanding IoT landscape. Potential applications include ride-sharing scooters, bikes, and smart home devices, further contributing to enhancing data privacy in a digitally connected society, including the automotive sector and beyond.

9. Conclusions

The proposed Vehicle Inactive Profile Remover (VIPR) framework addresses the growing privacy and security concerns associated with PII stored in connected automated vehicle infotainment systems. Our research confirmed that PII is often left unprotected, and a hands-on study revealed that prior renters' information could easily be accessed from multiple rental vehicles, posing serious privacy risks.

To better understand renters' awareness, we conducted a survey showing that most renters are unaware of their responsibility to delete data, with no automated solution currently available to assist them. VIPR fills this gap by automating the deletion of inactive profiles, ensuring data security for future renters.

Through extensive planning, analysis, mathematical models, and experiments using a Raspberry Pi, VIPR demonstrated its ability to seamlessly integrate with vehicle systems,

efficiently removing inactive profiles while preserving active ones. VIPR offers a practical, scalable approach to safeguarding data in the connected automated vehicle ecosystem, making it a significant advancement and underscores as a game-changer in the automotive cybersecurity industry.

10. Patents

Our commitment to innovation is further demonstrated by the patent filed with the United States Patent Office [28] for the integration of VIPR into existing connected vehicle software stacks. The patent signifies a key milestone in advancing data security within the automotive sector and serves as an essential step toward ensuring user privacy and security in an increasingly connected world.

Author Contributions: J.C. and H.M. made substantial contributions to the conception, design, and development of the VIPR, performed VIPR experiments, wrote the manuscript, and documented the final experiment results. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

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

References

1. Sanders, R.L. Car Renters Beware Bluetooth Use Can Reveal Your Private Data. *USA Today*, 30 January 2018.
2. Liang, J.; Li, Y.; Yin, G.; Xu, L.; Lu, Y.; Feng, J.; Shen, T.; Cai, G. A MAS-Based Hierarchical Architecture for the Cooperation Control of Connected and Automated Vehicles. *IEEE Trans. Veh. Technol.* **2023**, *72*, 1559–1573. [CrossRef]
3. Zhou, J.; Yang, K. A Parameter Privacy-Preserving Strategy for Mixed-Autonomy Platoon Control. *arXiv* **2024**, arXiv:2401.15561.
4. Capretto, A. *These Were the Top-Selling Vehicles in the USA in 2023*; CarBuzz: Miami, FL, USA, 2024.
5. Romjue, M. Annual U.S. Car Rental Revenue Tops Itself Again at $38.3 Billion. 2023. Available online: https://www.autorentalnews.com/10212500/annual-u-s-car-rental-revenue-tops-itself-again-for-2023-at-38-3-billion?utm_source=dlvr.it&utm_medium=linkedin (accessed on 28 August 2024).
6. Jones, P. Rental Car Demographic: 59 User Facts & Numbers [2023]. 2023. Available online: https://motorandwheels.com/rental-car-demographics-facts/ (accessed on 28 August 2024).
7. Jones, P. How Often Are Rental Cars Replaced? (Checked & Explained). 2022. Available online: https://motorandwheels.com/how-often-rental-cars-replaced/#:~:text=Here%E2%80%99s%20the%20Short%20Answer%20to%20How%20Often%20Rental,has%20no%20more%20than%2036,000%20to%2040,000%20miles. (accessed on 28 August 2024).
8. Lacroix, J. Vehicular Infotainment Forensics: Collecting Data and Putting It into Perspective. 2017. Available online: https://ontariotechu.scholaris.ca/items/40ba2fc3-f7ff-4c66-8a04-e388a11cf579 (accessed on 5 October 2024).
9. Walter, J.; Abendroth, B. On the role of informational privacy in connected vehicles: A privacy-aware acceptance modelling approach for connected vehicular services. *Telemat. Inform.* **2020**, *49*, 101361. [CrossRef]
10. Carlton, J. Security and Privacy Analysis on Personal Identifiable Information for Connected Commercial Vehicles. *Preprints* **2024**, 2024092195. [CrossRef]
11. Consumer Advice. *Renting a Car. Retrieved from Federal Trade Commission, Consumer Advice: Renting a Car*; Consumer Advice: London, UK, 2023.
12. GDPR; EP European Commission. *Retrieved from Data protection in the EU: Data Protection in the EU—European Commission*; European Commission: Brussels, Belgium, 2016.
13. CCPA; CA California Consumer Privacy Act (CCPA). *Retrieved from State of California Department of Justice: California Consumer Privacy Act (CCPA)*; Department of Justice, Office of the Attorney General: Sacramento, CA, USA, 2023.
14. Hannah Ji-Otto, L.; Kostas, S. *Cybersecurity and Privacy Concerns in Collecting Data from EV Drivers' Devices*; Baker Donelson: Atlanta, GA, USA, 2023.
15. Auto Remarketing Staff. *New App Claims to Wipe Personal info Left in Infotainment System*; Auto Remarketing: Birmingham, AL, USA, 2018.
16. Commission, F.T. The Connected Cars Workshop: The Federal Trade Commission Staff Perspective. 2018. Available online: https://www.ftc.gov/system/files/documents/reports/connected-cars-workshop-federal-trade-commission-staff-perspective/staff_perspective_connected_cars_0.pdf (accessed on 5 October 2024).
17. Gao, G.A. Vehicle Data Privacy Industry and Federal Efforts Under Way, but NHTSA Needs to Define Its Role. 2017. Available online: https://www.gao.gov/assets/gao-17-656.pdf (accessed on 5 October 2024).

18. 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): Gaithersburg, MD, USA, 2018.
19. Turner, A. Survey Reveals Privacy Concerns with Personal Data Left in Cars. AMOnline. 2024. Available online: https://www.am-online.com/news/survey-reveals-privacy-concerns-with-personal-data-left-in-cars#commentsection (accessed on 5 October 2024).
20. Palmer, D. Connected Cars: What Happens to Your Data after You Leave Your Rental Car Behind? ZDNET. 2017. Available online: https://privacyinternational.org/sites/default/files/2017-12/cars_briefing.pdf (accessed on 5 October 2024).
21. Privacy International. *Connected Cars: What Happens to Our Data on Rental Cars?* Privacy International: London, UK, 2017.
22. Lee, D.; Hess, D. Public concerns and connected and automated vehicles: Safety, privacy, and data security. *Humanit. Soc. Sci. Commun.* **2022**, *9*, 90. [CrossRef]
23. Carlton, J. Rental Car Mobile/Data Synchronization. 2023. Available online: https://forms.office.com/Pages/DesignPageV2.aspx?origin=NeoPortalPage&subpage=design&id=DQSIkWdsW0yxEjajBLZtrQAAAAAAAAAAAN__tcIcdVUNzhYT1VHNUtRQ0w3N0xSV0ZRMFdGTVFUQS4u&analysis=false (accessed on 5 October 2024).
24. Marius, P.; Toma, C.; Boja, C.; Alin, Z. Privacy and Security in Connected Vehicles Ecosystems. *Inform. Economica.* **2017**, *21*, 29–40. [CrossRef]
25. Renganathan, V.; Yurtsever, E.; Ahmed, Q.; Yener, A. Valet attack on privacy: A cybersecurity threat in automotive Bluetooth infotainment systems. *Cybersecurity* **2022**, *5*, 30. [CrossRef]
26. Hull, R. Are you giving away your personal data in your old car by mistake? What to watch out for. *This is Money*, 17 June 2024.
27. Pfleging, B.; Schneegass, S.; Schmidt, A. Multimodal interaction in the car: Combining speech and gestures on the steering wheel. In Proceedings of the 4th International Conference on Automotive User Interfaces and Interactive Vehicular Applications, Portsmouth, NH, USA, 17–19 October 2012.
28. Carlton, J.; Malik, H.; Shah, P. Vehicle 'Inactive' Profile Remover. US Patent No. 84555470, 1 April 2023.

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.