Carlton *et al. J Surveill Secur Saf* 2024;5:198-212
DOI: 10.20517/jsss.2024.07

Journal of Surveillance, Security and Safety

Original Article

Open Access

Check for updates

A data privacy survey on personal identifiable information (PII) left on rental vehicle infotainment systems

Jason Carlton, Hafiz Malik

Department of Electrical Engineering, University of Michigan Dearborn, Dearborn, MI 48128, USA.

Correspondence to: Dr. Jason Carlton, Dr. Hafiz Malik, Department of Electrical Engineering, University of Michigan Dearborn, 4901 Evergreen Rd, Dearborn, MI 48128, USA. E-mail: jcarlto@umich.edu; hafiz@umich.edu

How to cite this article: Carlton J, Malik H. A data privacy survey on personal identifiable information (PII) left on rental vehicle infotainment systems. *J Surveill Secur Saf* 2024;5:198-212. https://dx.doi.org/10.20517/jsss.2024.07

Received: 11 Mar 2024 **First Decision:** 30 Aug 2024 **Revised:** 20 Oct 2024 **Accepted:** 30 Oct 2024 **Published:** 9 Nov 2024

Academic Editors: Bomin Mao and Umit Karabiyik **Copy Editor:** Ting-Ting Hu **Production Editor:** Ting-Ting Hu

Abstract

In the current automotive ecosystem, the trend of pairing mobile devices to connected vehicles is gaining momentum, providing a vast number of benefits such as hands-free driving and remote vehicle control. However, along with these conveniences arises the issue of data accumulation, ranging from vehicle diagnostics to personal identifiable information (PII). The problem emerges when a consumer rents a vehicle, pairs their mobile device to the infotainment system, and neglects to remove their device prior to returning the vehicle. This oversight can potentially expose vulnerabilities with the current renter's PII for subsequent renters to exploit. Research indicates that renters often overlook the deletion process prior to returning the rental vehicle and are unaware of whose responsibility it is to perform this task. In this survey, we investigated the experiences and perceptions of a group of consumers who have previously rented vehicles. We wanted to know if the participants were aware they were responsible for deleting their mobile device from the rental vehicle before returning it, the renters' importance and tolerance for risk if they overlooked the deletion process leaving their shared data on the infotainment system for subsequent users, and if they were aware who was responsible for deleting their shared data. Lastly, we explored if the participants supported an automated solution to perform this manual deletion process. The goal of this paper is to demonstrate the significance of safeguarding PII in connected vehicles and advocate for the adoption of an automated solution to mitigate this privacy risk.

Keywords: Connected vehicles, data privacy, data security, ride sharing, rental vehicles, personal identifiable information (PII), infotainment system

INTRODUCTION

In the ever-evolving landscape of connected vehicles, automotive manufacturers have introduced cutting-edge software technology to remotely access a vast array of services such as unlocking and starting the vehicle, adjusting seats, personalizing climate control, scheduling service, and more. Today's modern vehicles also come equipped with embedded systems that communicate over short distances with other vehicles [vehicle-to-vehicle (V2V)], infrastructure [vehicle-to-infrastructure (V2I)], pedestrians [vehicle-to-pedestrian (V2P)], etc., in an ecosystem known as vehicle-to-everything (V2X), as shown in Figure 1.

While these advancements are beneficial, critical concerns arise on the potential vulnerabilities generated with the large amounts of data collected by connected vehicles. This can possibly give adversaries additional attack surfaces to exploit personal identifiable information (PII) of consumers. According to an article published by Wejo, "With millions of vehicles connected to the internet, the amount of data generated is massive, enabling valuable insights into the behavior of drivers as well as the state of the roads"[1].

In most recent news, an article published by the federal government states, "Concerns regarding how connected vehicles use and provide access to consumer and automotive data were top of mind across the federal government this week, spurring multiple developments including two new rulemaking proceedings at the Department of Commerce (Commerce) and the Federal Communications Commission (FCC or Commission) and a congressional request for additional action by the Federal Trade Commission (FTC)"[2]. Therefore, we scoped our research and contributions to consumers' renting vehicles in the United States market.

The issue in the rental market is when a renter links their mobile phone to the rental vehicle's infotainment system and overlooks performing the deletion process prior to returning it to the rental depot; by neglecting this crucial step, it exposes vulnerabilities on the current renters PII to subsequent renters. According to an article from the FTC, "a rental car with these features might keep your personal information long after you've returned the car. This information might include locations you put into your GPS - like where you work or live, your phone number, call and message logs, or even contacts and text messages. Unless you delete that data before you return the car, future renters or rental car employees may be able to see it."[3].

We conducted a survey to a group of participants with firsthand experience renting a vehicle with the goal being to gain insights into the following questions:

(1) During the transaction process, were they presented with or educated on the rental companies' privacy policies?

(2) Do they know who is responsible for expunging their data from the rental vehicle prior to its return? And for subsequent rentals?

(3) How do they rate their risk tolerance if the shared data is seen by subsequent renters from overlooking the deletion process?

(4) How important is their personal information to them?

(5) Most importantly, would they support an automated solution to automatically unlink and delete their information?

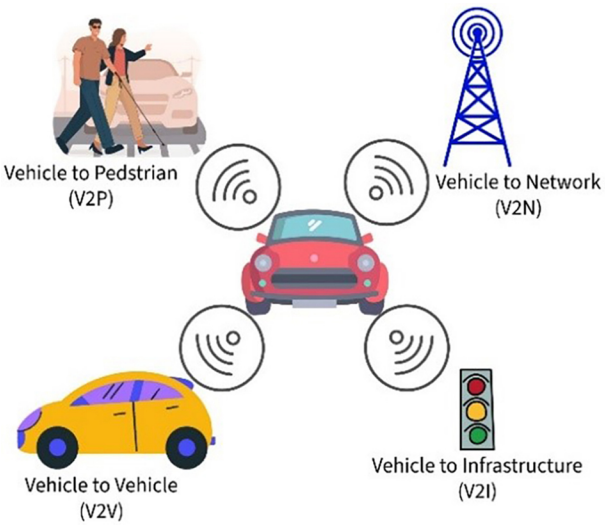

Figure 1. Key components of V2X. V2X: Vehicle-to-everything.

RELATED WORK

Privacy leakage in modern lifestyles

In today's connected world, PII is increasingly vulnerable due to the proliferation of smart devices, connected vehicles, wearable technology, etc. As individuals integrate more of these gadgets into their daily lives, the risks of PII leakage grow. The risks grow due to insufficient stringent privacy controls and the often-overlooked vulnerabilities that reside in these technologies. This section highlights research and some real-world incidents to demonstrate the privacy risks associated with modern digital lifestyle and its evolving ecosystems.

Wearable devices and privacy concerns

Wearable technology, such as fitness trackers, smartwatches, and smart glasses, has become an integral part of the modern digital lifestyle. These devices collect and store a wide range of sensitive data, including biometric, location, health, and behavioral patterns, raising significant privacy concerns if mishandled. Studies[4] suggest that many wearable devices lack strong security mechanisms, making them susceptible to unauthorized access, data breaches, and privacy leakage[5]. One real-world example is the Strava fitness app incident in 2018[6], where the app inadvertently exposed the locations of secret military bases through its global heatmap by displaying aggregated GPS data, including soldiers stationed at sensitive locations. This incident emphasized that wearables can unintentionally expose critical information. Another concern arises from the newest innovative idea with the introduction of wearable smart glasses, such as the Ray-Ban Stories developed by Ray-Ban in collaboration with Meta, formerly Facebook, which has raised significant privacy concerns. These glasses come equipped with cameras, microphones, and touch controls, allowing users to capture photos, record videos, and make hands-free calls. While these features enhance user convenience, they also present risks related to unauthorized surveillance and privacy leakage[7].

Connected vehicle and infotainment systems

Connected autonomous vehicles (CAVs) and rental cars in the automotive domain also have substantial risks to consumers' privacy. Specifically, infotainment systems in rental vehicles store personal data, such as phone contact lists, GPS locations, and call logs, without any proper deletion mechanisms. Privacy International[8] investigated car rental companies, such as Hertz and Europcar, and discovered that personal data from previous renters remain accessible in the vehicle's infotainment system. The personal data

included contact lists and location data that could be easily accessed by subsequent renters, presenting serious privacy risks due to the lack of automated data deletion protocols.

Given the increasing reliance on Internet-of-Things (IoT)-enabled vehicles and integration with personal devices, data left on these systems represents a significant threat to consumer privacy. The fact that personal data often remains after a vehicle has been rented by multiple renters calls for stronger measures in protecting PII, especially in high-turnover environments such as rental services.

Current approaches to privacy protection

In an attempt to address the privacy risks, several methods and tools have been developed to assist renters in managing their data on connected devices. For instance, Privacy4Cars[9] is 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. There have been additional measures and workshops conducted by government agencies, i.e., FTC and General Auditors Office (GAO).

For example, the FTC has recognized these emerging threats, especially in connected vehicles, where users unknowingly leave sensitive PII on infotainment systems. To address these challenges, the FTC convened a comprehensive workshop[10] focusing on mitigating security and privacy risks associated with connected vehicles. This workshop brought together key stakeholders from the automotive industry, government entities, and consumer advocacy groups. The primary outcomes from the workshop centered on three key areas.

(1) Better information sharing: Which suggests the importance of improved collaboration and information exchange between automotive industries, government entities, and other organizations involved in the connected vehicle ecosystem. Sharing insights and knowledge can help address emerging security and privacy challenges.

(2) Enhanced network design: This point underscores the need for developing network designs for vehicles that incorporate additional safeguards to protect consumers' PII. Strengthening security measures within the vehicle's network architecture is vital for ensuring data privacy.

(3) Risk assessment and mitigation: The reference to risk assessment and mitigation plans for connected vehicles highlights the importance of proactively identifying past, present, and future vulnerabilities and addressing them through measures such as over-the-air updates. This ongoing process is crucial for maintaining the security and privacy of connected vehicles.

Despite these approaches, the need for fully automated and user-friendly solutions remains critical, particularly in environments where frequent consumer turnover occurs, such as rental vehicles. Government initiatives, external studies[11], and regulations, such as the General Data Protection Regulation (GDPR)[12] in Europe and the California Consumer Privacy Act (CCPA)[13] in the United States, have attempted to provide frameworks for managing PII. However, these frameworks always lean towards manual processes; challenges in practical enforcement and technology adoption persist.

METHODOLOGY

Utilizing Office Forms, an Office 365 tool, we designed a survey titled "Rental Car Mobile/Data Synchronization"[14] to capture insights from consumers regarding personal information in the context of rental connected vehicles. The survey was conducted in April 2023 and aimed to explore the key areas and questions introduced earlier.

(1) Consumer awareness and education: Assessing knowledge of rental organizations' privacy policies.

(2) Deletion process: Investigating procedures to erase personal information from an infotainment system.

(3) Responsibility: Identifying the entity responsible for deleting personal information before vehicle return and re-rental.

(4) Consumer rating: Evaluating how consumers perceive and categorize shared personal information if retained on the rental vehicle's infotainment system.

(5) Interest in automation: Gauging interest in an automated solution to address these concerns.

After the survey was completed, we leveraged Google Colab for a quantitative data analysis. During the analysis, we incorporated various consumer scenarios to further explore the responses and insights in the results.

Responders

The survey was distributed to six hundred participants, with a target response rate of 20%, equivalent to 120 respondents. Out of these, five participants with no prior vehicle rental experience were excluded from the analysis, resulting in 115 participants, as detailed in Table 1. To ensure broad outreach, we deployed the survey across various social media channels such as Facebook, LinkedIn, and direct messaging. This strategy aimed to create a comprehensive and diverse respondent pool, laying the foundation for robust analysis while prioritizing respondent convenience.

RESULTS

Demographic information

The survey gathered some essential demographic data, specifically age groups categorized as (1) 18-24; (2) 25-34; (3) 35-44; (4) 45-54; and (5) > 54, along with gender. The survey results revealed notable insights into the theme of survey participants. The most prominent segment of the audience were men over the age of fifty-four, which represents a substantial 21.67%, and in the 35-44 age range, men also accounted for a significant 12.50% of the respondents, as illustrated in Figure 2.

Rental history

The survey also aimed to ascertain prior experience of participants with vehicle rentals and their engagement in consumer ride-sharing using their own vehicles through platforms such as Turo. Out of the total of 120 respondents, it was revealed that a substantial majority, 115 participants, had indeed engaged in vehicle rentals before. This is visually represented in Figure 3, which illustrates the widespread familiarity with rental services among the respondents.

Moreover, within this group of participants, a noteworthy insight emerged. Specifically, two individuals within the sample indicated their involvement in ride-sharing endeavors by utilizing their personal vehicles

Table 1. Demographic and key topics covered by respondents

	Demographics	U.S. count *N* = 120	U.S. percentage
Age range	18-24	2	1.67%
	25-34	18	15.00%
	35-44	28	23.33%
	45-54	20	16.67%
	> 54	52	43.33%
Gender	Man	68	56.67%
	Woman	47	39.17%
	Prefer not to say	5	4.17%
Rented vehicle before	Yes	115	95.8%
	No	5	4.2%
Connect mobile phone to vehicle	Yes	70	60.9%
	No	45	39.1%
Aware of rental organization privacy policies	Yes	14	12.2%
	No	59	51.3%
	Unsure	42	36.5%
Rate level of risk(1-5)	1	13	11.3%
	2	21	18.3%
	3	59	51.3%
	4	14	12.2%
	5	8	7.0%
Importance of shared information	Very important	44	38.3%
	Important	56	48.7%
	High	1	0.9%
	Not important	14	12.2%
If others can view information	Yes	98	85.2%
	No	17	14.8%
Aware to delet information	Yes	44	38.3%
	No	71	61.7%
Know how to delete information	Yes	32	27.8%
	No	55	47.8%
	Could Figure it out	28	24.3%
Responsible to delete information	Rental company	58	50.4%
	Renter	18	15.7%
	Both	2	1.7%
	Unsure	37	32.2%
Renter forgot to delete information prior to return	Yes	56	48.7%
	No	33	28.7%
	Unsure	26	22.6%
Automated solution to delete information	Yes	115	100.0%
	No	0	0.0%

to serve consumers via applications such as Turo. This compelling detail is visually illustrated in Figure 4, shedding light on the extent to which participants engage in this mode of consumer interaction.

Among the participants who have previous rental experience, an inquiry was made to ascertain the rental organizations they have utilized. Notably, the data reveals that Enterprise emerged as the predominant choice, as depicted in Figure 5.

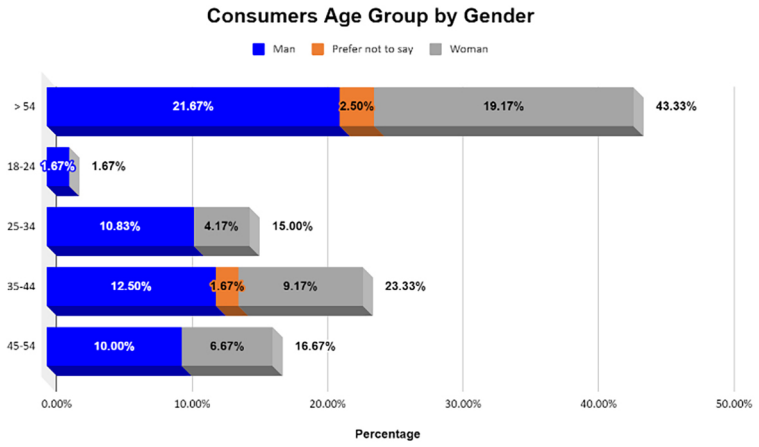

Figure 2. Participants age groups.

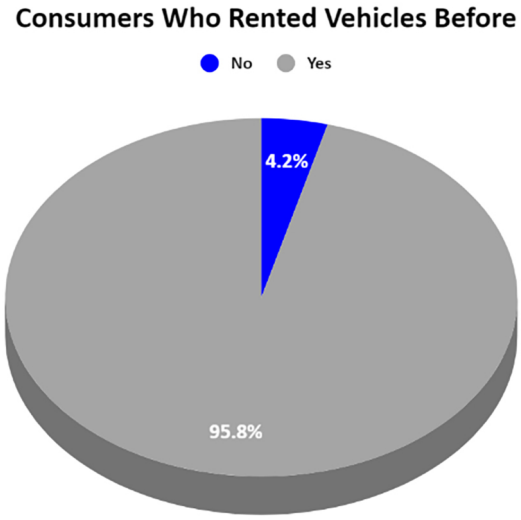

Figure 3. Participants who have prior rental experience.

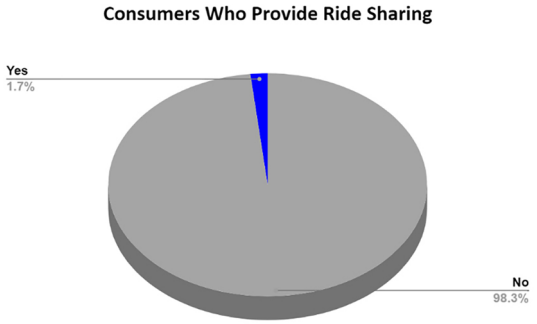

Figure 4. Consumers who utilize personal vehicles for ride sharing.

Furthermore, within the subset of respondents associated with ride-sharing services, both affirmed that they presented copies of the data privacy policies pertaining to the synchronization of mobile devices with vehicles. This suggests their commitment to safeguarding consumer information during such interactions.

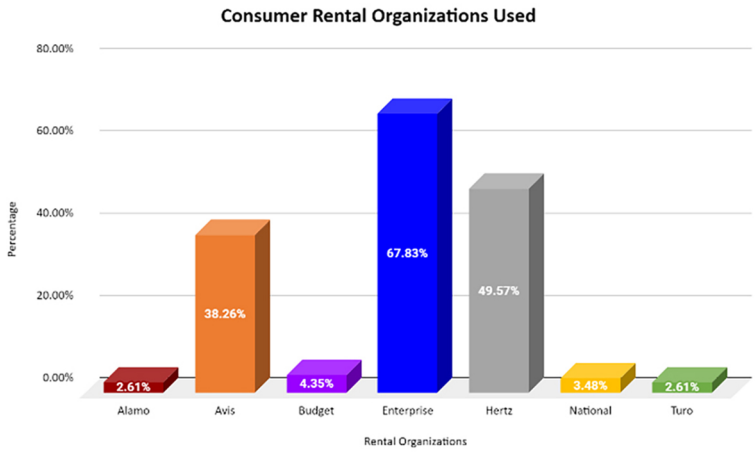

Figure 5. Consumers' rental organizations used.

Pairing and technology used in rentals

Out of the group with prior rental experience, there were revealing insights into their mobile phone pairing preferences and methods of pairing for those who elected to pair their mobile phones with rental vehicles, as shown in Figure 6. Within this group of participants (60.3%), the consumers expressed the various technologies used to pair with the vehicles. Most consumers use Bluetooth technology due to its short-range capabilities and ability to provide a driver distraction experience[15].

Mobile phone pairing choices

(1) 39.6% of participants opted not to pair their mobile phones with the rental vehicles they used.

(2) The majority, comprising 60.3% of participants, chose to pair their mobile phones with the rental vehicles.

Methods of mobile phone pairing

(1) A significant 57.6% employed a combination of cutting-edge technologies, utilizing both Bluetooth and USB connections for their pairing needs.

(2) A smaller subset, constituting 2.7% of participants, exclusively utilized USB connections for their mobile phone pairing.

These results offer valuable insights into the diverse preferences and technology adoption patterns among the participants with rental experience.

DISCLOSURE OF PRIVACY POLICIES AMONG PARTICIPANTS WITH RENTAL EXPERIENCE

Within the population of participants possessing prior rental experience, a significant lapse in privacy policy awareness during the transaction process is evident, as illustrated in Figure 7.

Awareness of privacy policies among consumers

(1) A substantial portion, accounting for 51.3% of consumers, reported not being informed about privacy policies during the transaction process, highlighting a notable absence of information.

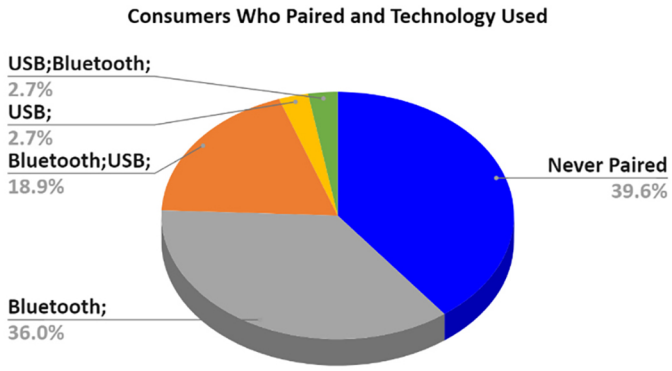

Figure 6. Consumers who paired and technology used.

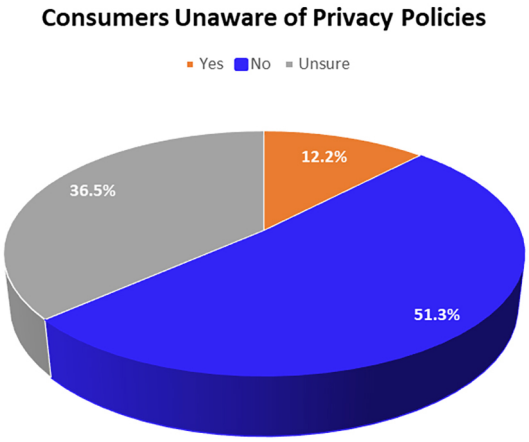

Figure 7. Consumers' awareness of privacy policies.

(2) A further 36.5% of respondents expressed uncertainty regarding their awareness of privacy policies, indicating a lack of clarity in this regard.

(3) A smaller group, constituting 12.2% of participants, confirmed that they were indeed made aware of the privacy policies during the transaction process, marking a comparatively smaller subset.

The findings are nothing short of astounding, shedding light on a critical issue: consumer awareness, or rather, the lack thereof, when it comes to privacy policies. Drawing from firsthand experience in renting vehicles, it becomes evident that vital information is often buried deep within these policies, particularly concerning whose responsibility it is to expunge profiles from infotainment systems before returning a rental vehicle.

What makes this situation even more remarkable is that due to consumers' unawareness of these policies, a substantial majority fail to take the necessary steps to delete their profiles prior to returning the rental vehicle. Therefore, valuable data remains on these vehicles, as depicted in Figure 8. These findings extensively illustrate the urgent need for greater transparency for the renter and education surrounding privacy policies in the realm of rental vehicles.

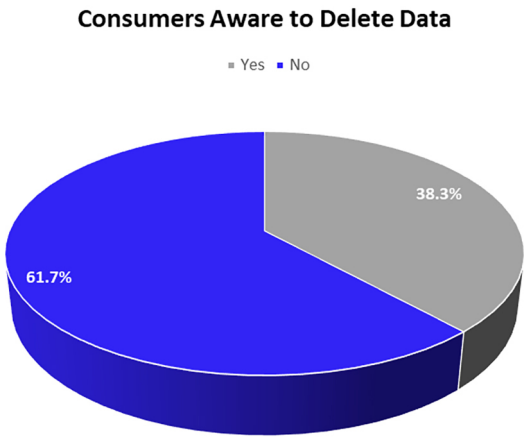

Figure 8. Consumer data expunged from rental vehicle.

Data risk and importance to consumers

In our pursuit of a more profound understanding of consumers' perspectives on the risks linked to sharing personal information through a rental vehicle's infotainment system, and the importance attached to retaining this data within the system, we have gained valuable insights from the participants. A substantial majority of respondents, precisely 70.5%, indicated a mid to higher perception of risk associated with sharing their personal information, as detailed in Figure 9. This exposes a prevailing awareness of the potential vulnerabilities and concerns related to data security in this context[16,17].

Furthermore, among the participants who expressed concerns about data security, an overwhelming 87.9% considered their personal information to be significant. This is reflected in their responses, categorizing the data as "important", "very important", or "highly important", as visually presented in Figure 10.

These findings underscore the significance of addressing data security and privacy concerns within the realm of rental vehicles, emphasizing the importance of safeguarding personal information, and fostering consumer trust in this technology-driven landscape.

Information not expunged from rental vehicle

Building upon the compelling responses from those who acknowledged a significant level of risk and classified their data as important or higher, we wanted to gain further insights into their willingness to permit data sharing in the event that their information was not deleted. Additionally, we aimed to understand consumers' knowledge regarding data deletion processes and whether they had ever forgotten to delete their data before returning the rental vehicle to the depot.

The results yielded remarkable findings. An astounding number of 85.2% of consumers expressed their concern about the possibility of their personal information being accessed by another individual, as depicted in Figure 11. This concerning unawareness constitutes a strong commitment to data privacy and a clear reluctance to allow unauthorized access to their information.

Furthermore, the survey revealed the intriguing observation of a significant majority of consumers admitting to being unfamiliar with the process of how to perform data deletion from a vehicle. However, a notable fraction expressed confidence in their ability to navigate this task, as indicated in Figure 12.

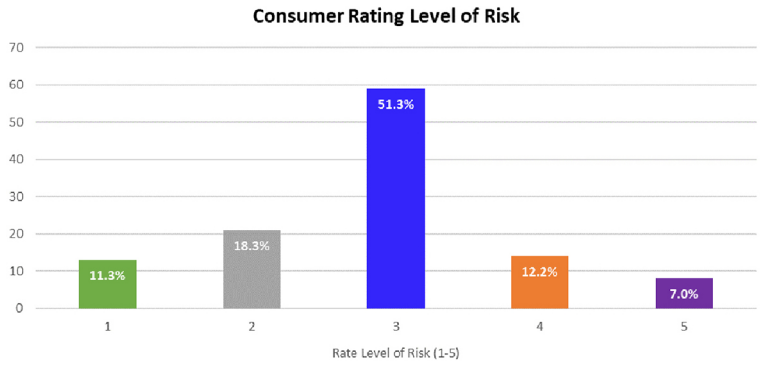

Figure 9. Consumers' risk level tolerance is risky at 70.5%.

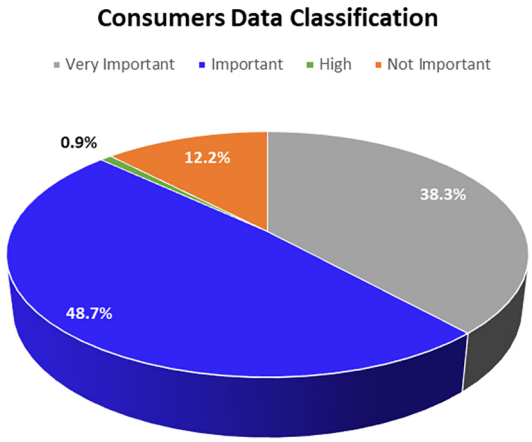

Figure 10. Consumers' data is extremely important at 87.9%.

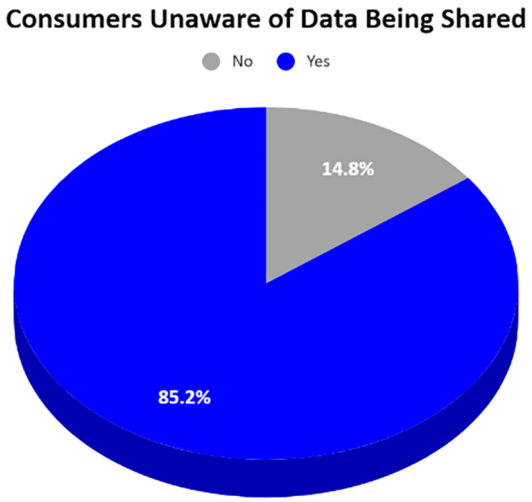

Figure 11. Consumers' awareness of data being shared.

These discoveries emphasize the critical importance not only of enhancing data security within rental vehicles but also of providing users with user-friendly tools and guidance for data deletion. The results

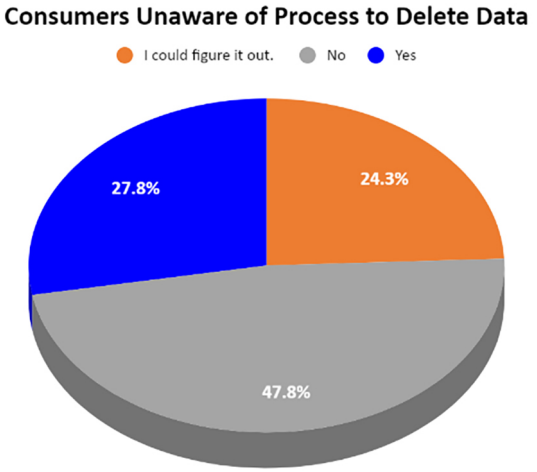

Figure 12. Consumers' awareness of process to delete data.

illustrate the significant responsibility that should be improved upon in the industry to bolster data privacy measures and to empower consumers with the knowledge and means to protect their personal information effectively.

Technology

Based on all the responses thus far for those who are in the process of expunging their data from a rental vehicle, it is notable that a significant portion either do not take action to delete their information or believe they could figure it out. Additionally, 71% of participants admitted to occasionally forgetting to delete their information from the infotainment system before returning the rental vehicle, as evident in Figure 13. This oversight has potential consequences, as it could leave sensitive data accessible to subsequent renters, potentially including location history, addresses, names, and family member details.

Remarkably, the majority of renters in the survey believed that the responsibility for data deletion lies with the rental organization, as depicted in Figure 14. This perception contradicts the fact that data privacy policies within rental organizations place the responsibility on the consumer to perform data deletion prior to return. This misunderstanding and lack of awareness contribute to data being inadvertently left on vehicles, thereby allowing subsequent renters to retrieve potentially sensitive information accessible through the infotainment system.

In response to this challenge, it is encouraging to observe that, as depicted in Figure 15, every participant expressed interest in and agreement with the idea of an automated solution to address this issue. This demonstrates collective support and consensus that an automated system would be a viable and effective means of mitigating data privacy risks associated with rental vehicles. It signals a clear desire for streamlined processes that safeguard data and protect consumer privacy more effectively.

DISCUSSION

In conclusion, the survey results shed light on significant gaps and misconceptions surrounding data privacy in the rental vehicle industry[18]. Notably, it is apparent that data privacy policies are often not presented to consumers prior to completing a rental transaction, potentially leaving them unaware of crucial details. There is a common misconception among renters that the responsibility for data deletion rests with the rental organization, even though such organizations' policies typically place this responsibility

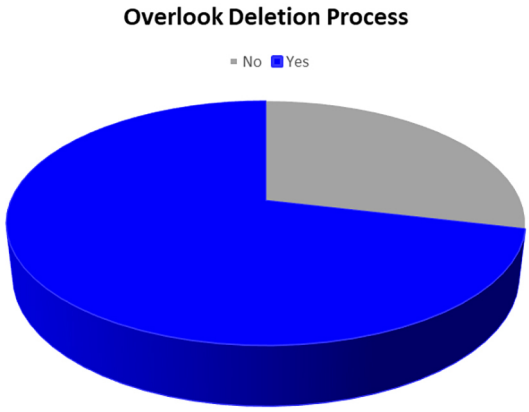

Figure 13. Consumers' overlook deletion process.

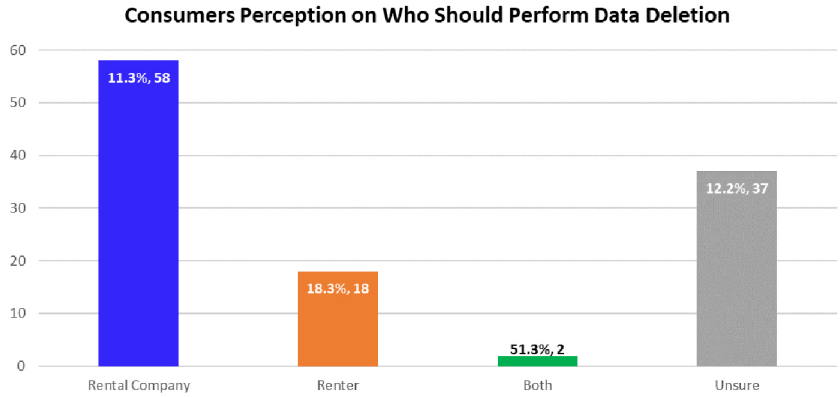

Figure 14. Consumers perception on who should perform data deletion.

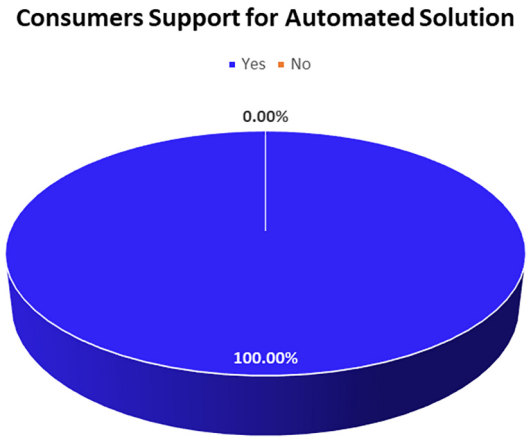

Figure 15. Consumers support automated solution for data deletion.

on the consumer. This gap in understanding poses a substantial security risk, as it could allow sensitive data to fall into the wrong hands, potentially endangering consumers. Additionally, the majority of respondents expressed unfamiliarity with the process of deleting their data from the infotainment system, further exacerbating the issue. Protecting PII is paramount to consumers, and the survey results make it clear that

they perceive their data as both important and at elevated risk.

As technology in vehicles continues to advance, with features such as V2V and V2I communication[19] and the rise of autonomous vehicles, the challenge of safeguarding data becomes even more complex. There was a striking consensus among the survey participants for the need of an automated technology solution to address these data privacy concerns. Such a solution could bridge the gap between consumers and rental organizations, offering a more robust safeguard for PII. In the pursuit of securing personal data and enhancing consumer trust, automated technology solutions are seen as a promising way forward. It is evident that addressing these challenges is a matter not only of data privacy but also of consumer safety and security in an increasingly interconnected world. This survey constituted a substantive step forward, poised to effect positive change and elevate the standards of data security and privacy for consumers utilizing rental vehicles equipped with advanced connected technologies.

Furthermore, building upon the research results and aiming to close the gap resulting from consumers' lack of awareness about data deletion processes, we developed an automated software to perform the deletion process for the renter (details to be provided in a forthcoming publication). Additionally, future research and development will need to address the following key areas:

(1) Education and awareness for consumers on data security and privacy: Initiatives to educate consumers about data security and privacy will be crucial. This includes raising awareness about the importance of safeguarding their personal information and understanding how data is managed in connected vehicles.

(2) Standardizing privacy policies among rental organizations: Efforts should be made to establish common standards for privacy policies among rental organizations. Standardization can help create consistency and transparency in data handling practices.

(3) Enhancing rental organizations' rental pick-up process: Rental organizations can play a pivotal role in ensuring consumer awareness of their privacy policies. Enhancements to the rental pick-up process can include informing renters about data handling and providing them with options for data removal.

(4) Continued technology enhancements for automated solutions: The development of automated solutions should be an ongoing process. Advancements in technology can lead to more efficient and effective methods for data removal and privacy protection.

By addressing these areas, we can better protect consumers' PII and ensure that they have the knowledge and tools to make informed decisions about their personal information when renting vehicles.

DECLARATIONS

Authors' contributions

Made substantial contributions to conception and design of the survey questions, coordinated the survey, composed the manuscript, and performed data analysis and interpretation: Jason C, Hafiz M

Availability of data and materials

The supporting data for this article is available upon request directly from the author.

Financial support and sponsorship
None.

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

Ethical approval and consent to participate
The survey included human participants, each of whom voluntarily participated anonymously, with no use of real names throughout the entire process.

Consent for publication
Not applicable.

REFERENCES

1. Semiconductor Engineering. Increased automotive data use baises privacy, security concerns. Available from: https://semiengineering.com/increased-automotive-data-use-raises-privacy-security-concerns/. [Last accessed on 9 Nov 2024].
2. JDSUPRA. Federal government acts on connected vehicle privacy and national security concerns. Available from: https://www.jdsupra.com/legalnews/federal-government-acts-on-connected-3574128/. [Last accessed on 6 Nov 2024].
3. Federal Trade Commission Consumer Advice. Renting a car. Available from: https://consumer.ftc.gov/articles/renting-car. [Last accessed on 6 Nov 2024].
4. Bouderhem R. Privacy and regulatory issues in wearable health technology. *Eng Proc* 2023;58:87. DOI
5. Khan F, Hwan K, Mathiassen L, Moore R. Data breach management: an integrated risk model. *Inf Manag* 2021;58:103392. DOI
6. Tait A. Fitness app Strava breached US security - it's time to consider the dangers of data. The New Statesman. Available from: https://www.newstatesman.com/science-tech/2018/01/fitness-app-strava-breached-us-security-it-s-time-consider-dangers-data. [Last accessed on 9 Nov 2024].
7. Wiak K. Smart glasses raise privacy concerns after Harvard experiment. Available from: https://www.msn.com/en-us/money/technology/smart-glasses-raise-privacy-concerns-after-harvard-experiment/ar-AA1rInFm?ocid=BingNewsVerp. [Last accessed on 6 Nov 2024].
8. Privacy International. Connected cars: what happens to our data on rental cars? Available from: https://privacyinternational.org/sites/default/files/2017-12/cars_briefing.pdf. [Last accessed on 6 Nov 2024].
9. Auto Remarketing Staff. New app claims to wipe personal info left in infotainment system. Available from: https://www.autoremarketing.com/ar/technology/new-app-claims-wipe-personal-info-left-infotainment-system/. [Last accessed on 6 Nov 2024].
10. Commission Federal Trade. The connected cars workshop: the federal trade commission staff perspective. Available from: https://www.ftc.gov/system/files/documents/reports/connected-cars-workshop-federal-trade-commission-staff-perspective/staff_perspective_connected_cars_0.pdf. [Last accessed on 6 Nov 2024].
11. Pesé MD, Shin KG. Survey of automotive privacy regulations and privacy-related attacks. Available from: https://www.researchgate.net/profile/Mert-Pese/publication/332157073_Survey_of_Automotive_Privacy_Regulations_and_Privacy-Related_Attacks/links/5e067c9f4585159aa49f800c/Survey-of-Automotive-Privacy-Regulations-and-Privacy-Related-Attacks.pdf. [Last accessed on 6 Nov 2024].
12. ROB BONTA Attorney General. California Consumer Privacy Act (CCPA). Available from: https://www.oag.ca.gov/privacy/ccpa. [Last accessed on 6 Nov 2024].
13. European Commission. Data protection in the EU. Available from: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en. [Last accessed on 6 Nov 2024].
14. Carlton J. Rental car mobile/data synchronization. Available from: https://forms.office.com/Pages/DesignPageV2.aspx?subpage=design&FormId=eruQyfRRm0O9NpwH-xBBwGUHkrwDaq1EqGYKQq0_fwxUNk4zS0wwTDBVOENZVDkwSElMOVhNRVlPVC4u&Token=c86d7a027980440daa43e93b982c6dbb. [Last accessed on 8 Nov 2024].
15. GHSA. Distracted driving. Available from: https://www.ghsa.org/state-laws/issues/distracted%20driving. [Last accessed on 6 Nov 2024].
16. Lee D, Hess DJ. Public concerns and connected and automated vehicles: safety, privacy, and data security. *Humanit Soc Sci Commun* 2022;9:90. DOI
17. Popa M, Toma C, Boja C, et al. Privacy and security in connected vehicles ecosystems. *Inform Econ* 2017;21:29-40. DOI
18. Carlton J. Security and privacy analysis on personal identifiable information for connected commercial vehicles. *Preprints* 2024:2024092195. DOI