Poster: What Are Cars Collecting? A Study of Privacy Policies in the Automotive Industry

Lachlan Moore
Waseda University
NICT

Rei Yamagishi
Waseda University

Kenji Sawada
Osaka University

Tatsuya Mori
Waseda University
NICT
RIKEN AIP

1 Introduction & Motivation

As modern vehicles evolve into highly connected, sensor-rich platforms, they increasingly resemble rolling computers on wheels. These advancements enable features such as advanced driver assistance, predictive maintenance, remote vehicle management, and personalized in-cabin experiences. However, these same systems also introduce serious privacy risks, as vehicles now collect and transmit a wide range of sensitive data—including precise location history, driving behavior, in-cabin audio, biometric identifiers, and personal contact lists. For example, vehicles may record facial recognition data for driver authentication, monitor speech for voice commands, or log frequent destinations and driving patterns.

These capabilities raise important questions about how such data is collected, stored, shared, and whether users, both drivers and passengers, are aware of or able to control these practices. Bloom et al. [2], who found that users are often uncomfortable with autonomous vehicle data collection and are willing to spend significant time managing or opting out of such practices. This suggests a disconnect between user expectations and real-world data collection mechanisms.

Previous studies have also shown that privacy policies across digital services are often opaque, too complex, or do not adequately communicate data practices to users [1, 4]. In the automotive domain, this problem is compounded by the fact that users may not even realize that traditional vehicles have become data-rich platforms. The regulatory landscape for vehicle data collection is still evolving [3], making it critical to assess whether current privacy policies reflect best practices in transparency and user empowerment.

To address these concerns, we performed a structured analysis of the U.S. privacy policies of 17 major vehicle manufacturers. Our goal is to identify what types of data are being collected, how it is shared (particularly with third parties), what rights, if any, users have to control or opt out of this collection, and data collection of non-primary drivers. Privacy policies are the primary (and often the only) documents that manufacturers provide to inform users about their data practices. Therefore, a policy-level audit offers a practical and necessary lens through which to understand the current state of privacy in the vehicle ecosystem.

2 Method

To ensure a consistent basis for comparison, we focused exclusively on U.S. privacy policies of vehicle manufacturers. We selected the largest and most prominent manufacturers operating in the U.S. market. Although these companies are active in the U.S., their global origins span multiple countries, including Japan (5), Germany (4), the United States (3), South Korea(2), Sweden (1), and the Netherlands (1). Our analysis began by collecting primary privacy policy documents from each manufacturer's official website. We then gathered all supplementary materials referenced or linked within those policies, including documents specific to connected services, mobile applications, individual vehicle models, and affiliated subsidiaries. Which consisted of 34 total documents. From these documents, we extracted four key elements: Types of data collected, user rights (e.g., opt-in/opt-out), data sharing practices (i.e., with whom the data is shared), and data collection of non-primary users (e.g., passengers and other drivers). Given the wide variation in format, we performed manual coding analysis of data collection practices into 11 standardized categories which are shown in Table 1.

3 Analysis

Type of Data Collected. Table 1 presents an overview of the data collection practices across 17 major vehicle manufacturers. Many manufacturers publish multiple privacy policies: a general privacy policy and one or more supplementary policies focused on domains such as connected vehicle services, mobile applications, or individual vehicle models. From the differences between the type of data collected, we can effectively assume the type of data collected by the vehicle. Which allows us to infer what vehicles often collect, including geolo-

Table. 1: Overview of data types stated as collected in each manufacturer's privacy policy. Both general and vehicle-specific policies are included when available. ∼ Indicates data not explicitly listed but mentioned elsewhere in the policy.

Vehicle Company	Audi	BMW	GM	Ford		Stellantis		Hyundai (Genesis, and Ioniq)		Honda/Acura		Kia		Mazda	Mercedes		Mitsubishi		Nissan	Subaru		Tesla	Toyota/Lexus		Volksw agen	Volvo	
Privacy Policy Type General - (G), Vehicle - (V)	G	G	G	G	V	G	V	G	V	G	V	G	V	G	G	V	G	V	G	G	V	G	G	V	G	G	V
Personal Information	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Sensitive Personal Information	✓	✓	✓	✓		✓	✓	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Commercial Information	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓		✓	✓	✓	✓
Biometric Information	✓					✓	✓	✓	✓						✓			✓			✓			✓		✓		
Network/Device Activity Information	✓	✓	✓	✓		✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓
Geolocation Information	✓	✓	✓	✓	✓		✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓
Sensory Information	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	~	✓				✓		✓	✓		✓	✓	✓			
Background Information	✓	✓				✓	✓	✓		✓		✓		✓	✓		✓	✓				✓	✓		✓	✓		
Inferences	✓	✓		✓			✓	✓		✓		✓	✓	✓						✓					✓	✓		
Driver Behavior Information	✓	✓	✓	✓	✓		✓	✓	✓		✓		✓	✓		✓			✓		✓			✓	✓		✓
Vehicle Information	✓	✓	✓	✓	✓		✓	✓	✓		✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓

cation, vehicle and driver information, sensory information, and, in some cases, even biometric information.

Transparency. Manufacturers with multiple brands, such as Hyundai and Toyota, often use distinct policies for each brand, service, or product. For example, Toyota and Lexus each have separate documents covering general data practices, app-specific policies, and model-specific disclosures. Although this may allow for more tailored communication, it also adds complexity to the privacy landscape that can overwhelm users and obscure a clear understanding of how their data is handled.

Data sharing practices. Data sharing practices revealed that 16 out of 17 manufacturers share user data with third parties. Tesla appears to be an exception, stating that it only shares data with authorized third parties. Toyota/Lexus stands out for claiming to share only anonymous data externally.

User rights. User rights and opt-out options within the privacy policies are limited. Opt-out options are often tied to regional regulations, such as the California Consumer Privacy Act (CCPA), and do not necessarily apply to all users. In many cases, opting out requires disabling connected services altogether or requesting data deletion, limiting access to vehicle features. Some manufacturers require users to go through additional steps, such as vehicle resets or direct contact with customer service, making the opt-out process even more cumbersome.

Data collection of non-primary users. The privacy policies we analyzed often briefly address how data from non-primary users, such as additional drivers or passengers, is handled, but the level of clarity and responsibility varies significantly. We identified three common patterns across manufacturers: (1) manufacturers state they collect such data but place the burden of notification on the vehicle owner (Ford, Stellantis, Hyundai, Kia, Toyota, Mitsubishi, Nissan); (2) manufacturers acknowledge collection without explaining how the data is used (Audi); and (3) some are unclear or vague about both collection and usage practices (Honda, BMW, Mazda, Mercedes, Subaru, Tesla, Volvo, Volkswagen).

4 Conclusion and Future Work

We provide a policy-level snapshot of how major vehicle manufacturers disclose data collection, sharing, and user rights. By categorizing the types of data collected and evaluating opt-out mechanisms, we identify trends, inconsistencies, and potential transparency gaps across the industry.

Our next steps include conducting a user study, inspired by previous work on autonomous vehicle perceptions [2], to assess the perceptions of individuals on current data collection practices of vehicle manufacturers. We also plan to investigate whether vehicles are, in fact, collecting the data described in their privacy policies through technical analysis or field studies. We aim to engage with vehicle manufacturers to share our findings and explore opportunities to improve transparency, communication, and user trust.

Acknowledgments

This work was supported by JST SPRING, Grant Number JPMJSP2128.

References

[1] R. Amos, G. Acar, E. Lucherini, M. Kshirsagar, A. Narayanan, and J. Mayer. Privacy policies over time: Curation and analysis of a million-document dataset. In *Proceedings of the Web Conference*, page 2165–2176, 2021.

[2] C. Bloom, J. Tan, J. Ramjohn, and L. Bauer. Self-driving cars and data collection: Privacy perceptions of networked autonomous vehicles. In *Proceedings of the Thirteenth Symposium on Usable Privacy and Security*, pages 357–375, 2017.

[3] K. Kemp. Driving blind: The unexamined privacy risks of connected cars. 2024.

[4] T. Linden, R. Khandelwal, H. Harkous, and K. Fawaz. The privacy policy landscape after the GDPR. In *Proceedings on Privacy Enhancing Technologies*, page 47–64, 2020.