Getting Consent From Drivers on the Go: A Privacy Consent Collection Framework for In-vehicle Systems

Tong Liu, Yuankun Li, Yuru Liu
Advised By Lorrie Cranor, Sponsored By HERE
Carnegie Mellon University
Privacy Engineering Capstone Project, Fall 2017
Executive Summary

1. Challenge

HERE Technologies, a digital location technology company that provides location-based services to various verticals, including Automotive, has been considering different means of acquiring consent in an in-vehicle context. Dependent on the use case, regulations such as General Data Protection Regulation (GDPR) may require HERE to obtain consent from drivers before collecting their data for navigation services. However, HERE does not have a direct relationship with drivers. HERE's clients are vehicle manufacturers, and HERE provides their navigation service through SDKs to different vehicle manufacturers. Vehicle manufacturers design their own in-vehicle navigation systems based on the SDKs. HERE's privacy notices need to be made available on the in-vehicle navigation system, to ensure drivers are informed about the collection and use of their data. Drivers are usually not fully be aware of parties that provision in-vehicle services, including navigation services, especially in connected vehicles. Therefore, it is challenging to ensure appropriate transparency with the data subject (drivers and/or other individuals) and to acquire consent from them, where necessary. Nonetheless, it becomes important to have an effective interface to communicate with drivers and obtain consent, where legally required.

Gaining in-vehicle consent is challenging. First, the in-vehicle display is too small to convey a full privacy policy effectively, so the solution has to either redirect drivers to another display method or find a way to convey a long policy on a small screen. In addition, drivers are usually in a rush to use the navigation system, and want to start driving as soon as possible. If the consent process is too time-consuming, drivers would find it annoying and may just ignore the process. The consent process also needs to be flexible enough to accommodate multiple options, including a private mode in which no personal data would leave the vehicle or no personal data would be processed in the first place. In addition, establishing consent from drivers is not a one-time event at purchase time. This is because consent will need to be obtained from every driver of the vehicle, and it will need to be obtained again if the navigation provider decides to use the data in a different way. Thus, the solution should be able to trigger the consent process as needed. The consent solution we propose should meet all these requirements.

2. Consent Framework

Based on the above problem statement, we came up with several ideas that could be used to trigger the consent process or to communicate with drivers. We proposed a consent framework including four different methods to collect consent from drivers in an in-vehicle context, as shown in Figure 1.

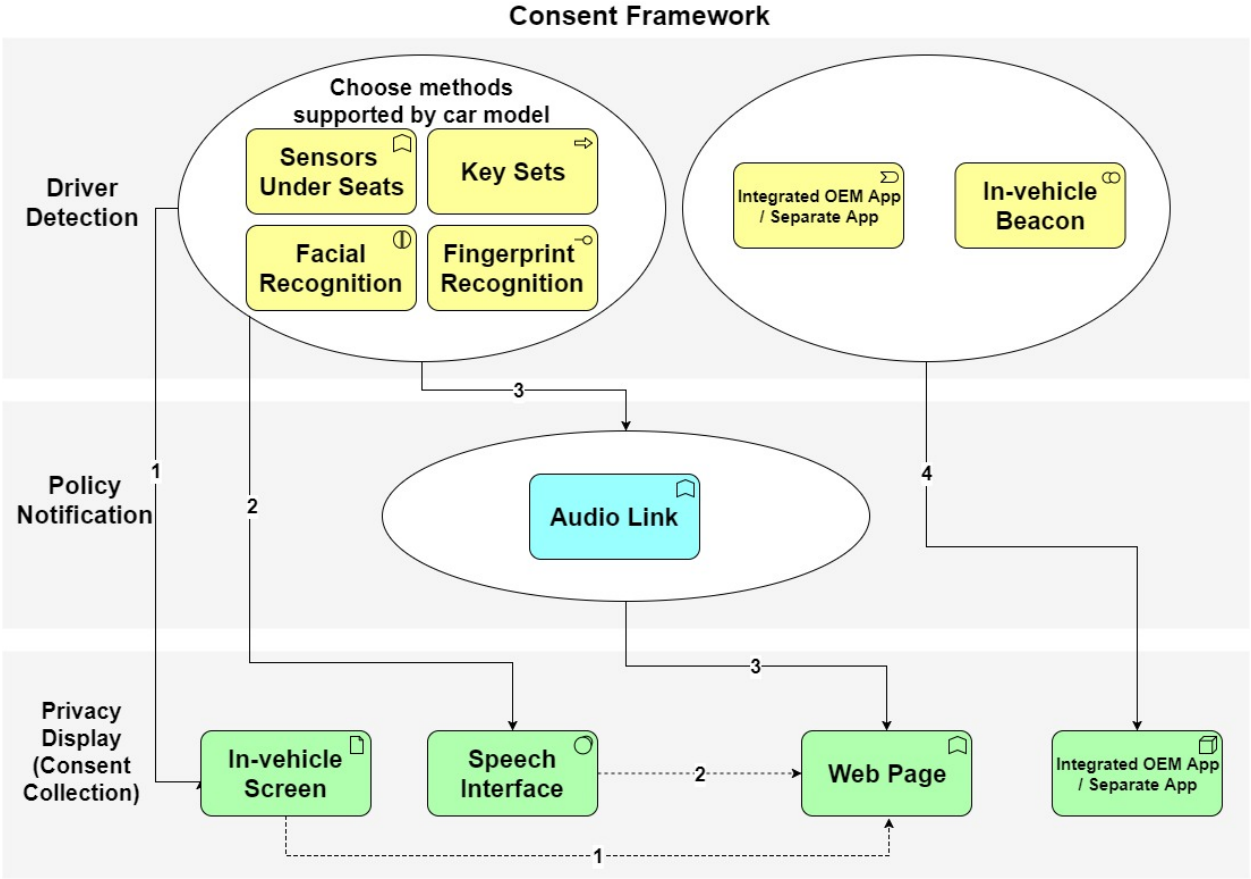

Figure 1. Consent Framework Flowchart

In-vehicle Screen

Vehicle hardware, such as sensors under seats or facial recognition, are used to detect new drivers. When a new driver is found, the In-vehicle screen is triggered to display a privacy notice that includes a concise version of the privacy policy. Drivers can read the privacy notice and give consent through the in-vehicle screen. In addition, a QR code and a URL that could redirect drivers to the full privacy policy website are displayed on the screen.

Speech Interface

In-vehicle biometric sensors, such as weight sensors under seats or cameras with facial recognition, are used to detect new drivers. When a new driver is found, an in-vehicle speech interface will interact with drivers. During this process, the speech interface will introduce the privacy policy, and the driver can give consent by saying “yes” or decline by saying “no.” The

speech interface can provide a URL to the full privacy policy website to drivers who make such request.

Audio Link

In-vehicle biometric sensors, such as weight sensors under seats or cameras with facial recognition, are used to detect new drivers. When a new driver is detected, the in-vehicle audio interface will play a tone that encodes a URL. T Drivers can uses their phone to receive this tone. The phone navigates automatically to a web page corresponding to the transmitted URL. Finally, the driver reads the privacy policy and may gives consent on the web page.

Independent/Integrated App

Drivers install an app on their phone. This app proactively detects the in-vehicle system through Bluetooth. When a vehicle is detected, the app will detect whether this vehicle is new for this app. If yes, this driver needs to give consent to use this vehicle. The app can automatically display the privacy policy and consent form and obtain the driver's consent. The app may be an integrated app provided by the vehicle manufacturer, or an independent app that could be used with cars from many manufacturers.

3. User Study And Results

We evaluated the effectiveness of and user preference for each method in the consent framework through a two-part user study. The first part was a lab study and the second part was an online survey that was deployed through Amazon Mechanical Turk (MTurk). For both parts, we recruited participants who own cars.

The lab study was a one-hour within-subject study. For each action flow, participants watched a demo video to illustrate the concept and process. Participants then answered multiple choice questions, including questions about hypothetical scenarios. For each question, they were asked to explain their answers. In the online survey, participants were asked to watch the demo videos and answer multiple choice questions, similar to the procedure in the lab study.

Results

Overall, our survey results are consistent with our lab study results. The in-vehicle screen is the most favored method for giving consent, and the audio link is the least favored. Most participants agreed that the in-vehicle screen is easy to understand, and they are already accustomed with using in-vehicle screens to interact with cars. As the most common and traditional method, the in-vehicle screen method did not receive many negative comments during the user study. The speech interface method received quite diverse comments. While some participants really liked the idea that they don't have to stare at any screen and felt that having a conversation with the system is less distracting, some people found the audio guidance intrusive and slow. As for the audio link and the integrated/independent app method, most participants expressed concerns about using an app to gain consent. They find it

unnecessary to involve their phones in an in-vehicle activity, and stated that drivers don't always have their phones with them during driving, though, some participants thought the independent/integrated app methods was fast, simple, and straightforward.

In the end, we have come to conclusion that Gaining in-vehicle consent is challenging due to many limitations of the environment and the relationship between service providers and OEMs. Hence, the solutions we proposed in the consent framework all have their pros and cons. Overall, the in-vehicle screen is the most favored method because it is the most common and natural way to obtain consent, though some participants still think it is time-consuming in typical cases. Other methods such as speech interface and app based solution, tested in the user study are promising as well.