Researcher: Your car might be watching you to keep you safe, at the expense of your privacy

December 6 2023, by M. Hadi Amini

Credit: Unsplash/CC0 Public Domain

Depending on which late-model vehicle you own, your car might be watching you—literally and figuratively—as you drive down the road.

It's watching you with cameras that monitor the cabin and track where you're looking and with sensors that track your speed, lane position and rate of acceleration.

Your car uses this data to make your ride safe, comfortable, and convenient. For example, the cameras can tell when you've been distracted and need to bring your attention back to the road.

They can also identify when you are speeding by verifying the speed limit from your GPS position or traffic signs along the road and warn you to slow down. Some carmakers are also beginning to incorporate similar features for convenience, such as unlocking your car by scanning your face or fingerprint.

Your car may also transmit some of this data to the manufacturer's data centers, where the company uses it to improve your driving experience or provide you with personalized services.

In addition to providing these benefits, this data collection is a potential privacy nightmare. The information can reveal your identity, your habits when you're in your car, how safely you drive, where you've been, and where you regularly go. A report by the Mozilla Foundation, a nonprofit technology research and advocacy organization, found that carmakers' privacy policies are exceedingly lax.

The study identified cars as the "worst category of products for privacy that we have ever reviewed." U.S. Sen. Ed Markey wrote a letter to U.S. automakers on Nov. 30, 2023, asking a lengthy set of questions about their data practices.

Today's smart cars present drivers with a trade-off between convenience and privacy, assuming drivers have the option of improving the data privacy of their cars. As a computer scientist who studies cybersecurity

and resilience in transportation, I see several technological routes to getting the best of both worlds: cars that make use of this collected data while also preserving users' privacy.

Driver data

Today's cars use a wide range of sensors to understand the environment, analyze the data and ensure the safety of passengers. For instance, cars are equipped with sensors that measure brake pedal position, vehicle speed, driver's movements, surrounding vehicles and even traffic lights. The collected data is transmitted to the car's electric control units, the computers that operate the car's many systems.

There are two types of sensors that continuously monitor and predict a driver's drowsiness. The first is vehicle status monitoring sensors such as lane detection and steering wheel position tracking. This data is not directly related to a specific person and can be considered not personally identifiable information unless it is correlated with other data that identifies the driver.

The second type of sensor tracks the drivers themselves. This category includes things like cameras to track the driver's eye movements to predict fatigue. This second group of sensors is directly related to the driver's privacy because they collect personally identifiable information, such as the driver's face.

Protecting privacy

There is a trade-off between the quality of the driving experience and the privacy of drivers, depending on the level of services and features. Some drivers may prefer to share their biometric data to facilitate accessing a car's functions and automating a major part of their driving experience. Others may prefer to manually control the car's systems,

sharing less personally identifiable information or none at all.

At first glance, it seems the trade-off of privacy and driver comfort cannot be avoided. Car manufacturers tend to take measures to protect drivers' data against data thieves, but they collect a lot of data themselves. And as the Mozilla Foundation report showed, most car companies reserve the right to sell your data. Researchers are working on developing data analytics tools that better protect privacy and make progress on eliminating the trade-off.

For instance, over the past seven years, the concept of federated machine learning has attracted attention because it allows algorithms to learn from the data on your local device without copying the data to a central server. For instance, Google's Gboard keyboard benefits from federated learning to better guess the next word you are likely to type without sharing your private data with a server.

Research led by Ervin Moore, a Ph.D. student at Florida International University's Sustainability, Optimization, and Learning for InterDependent Networks laboratory, and published in *IEEE Internet of Things Journal* explored the idea of using blockchain-based federated machine learning to improve the privacy and security of users and their sensitive data. The technique could be used to protect drivers' data. There are other techniques to preserve privacy as well, such as location obfuscation, which alters the user's location data to prevent their location from being revealed.

While there is still a trade-off between user privacy and quality of service, privacy-preserving data analytics techniques could pave the way for using data without leaking drivers' and passengers' personally identifiable information. This way, drivers could benefit from a wide range of modern cars' services and features without paying the high cost of lost privacy.