Professional Perspective

Connected Vehicles & Automatic Decision-Making

Jean Paul Yugo Nagashima, Frost Brown Todd

Bloomberg Law

Connected Vehicles & Automatic Decision-Making

Contributed by Jean Paul Yugo Nagashima, Frost Brown Todd

Connected cars are the next step to bringing mobility to everyone. Automotive companies have claimed that more than a half-dozen cars sold in 2021 were considered almost self-driving. The 2021 Infrastructure Investment and Jobs Act requires new cars built after 2026 to implement systems to passively monitor the drivers' performance to detect drunken driving. H.R. 3684 §24220. Some of the proposed technologies monitor the drivers for signs of impairment through built-in cameras of the car's interior.

Eliminating drunk drivers on the road is a sound policy. However, monitoring drivers and allowing cars to prohibit driving raise privacy and autonomy questions. Should behaviors like speeding be automatically monitored for chronic violators of speeding tickets for purposes of traffic safety? As more automated decisions are made from the data collected from connected cars, this policy starts to resemble the contours of the social credit system. This article focuses on conflicts the automotive industry will face—between government policies requiring automated decision-making and the rise in data privacy laws that protect consumers from certain data collection and subject them to automatic decision-making.

Social Credit Scoring System

The social credit score system is a credit rating system that attempts to link public and private data on financial and social behavior of individuals and entities and to track and evaluate their trustworthiness. China originally developed this concept to combat financial fraud and non-compliance of civil court judgments during the mid-2000s. China first rolled out this system in 2014 and has rated individuals in China to place them on a blacklist or a whitelist depending on the individual's social credit score.

The social credit score system is built on two parts: data collection, and reward and punishment based on the credit score. Data collection is performed on a multitude of monitoring systems. Although the exact methods for the evaluation are kept secret, credit information, purchasing behavior, criminal background, compliance with court or administrative orders, traffic violations, online behavior, and actions in public are collected. Any information or behavior that is considered negative leads to an individual receiving a lower score, and behavior considered positive will increase the score.

The social credit score system then implements a punishment reward system depending on the individual's score. Chinese authorities have used social credit to ban individuals from purchasing flights, making reservations on high-speed express trains, or staying at a luxury hotel. This has also impacted the day-to-day lives of individuals. For alleged bad behaviors of playing too many video games, authorities have throttled the internet speed of households with chronic gamers.

The punishment could also take more severe forms like denying entrance into a university or employment. However, if an individual has a high social credit score, the authorities may provide perks. For example, high-score individuals receive a discount on energy bills, book a hotel without a deposit, or even "boost" their user profile on a Chinese dating site. In other words, the social credit score system uses a "carrot and stick" approach to induce a desired behavior from the individuals.

Data Collection & Decision-Making Implications

Social credit score-type systems may sound far-fetched in the U.S. But, if connected vehicles can collect driver's behavioral data for purposes for impairment under the infrastructure law, it opens the possibility for rules and regulations that may penalize drivers for their consolidated bad driving behavior, just like social credit scores. A connected vehicle's data collection may determine that the driver routinely drives over the speed limit and may decide to throttle the car's speed for safety reasons. This may look as though it is a reasonable algorithmic decision. However, when allowing algorithmic decision-making in cars, the automotive industry should be aware of two issues:

- Does the car (or the car company) have a legitimate reason to collect and use the car speed information, such as driver's consent?
- Should algorithmic decision-making be implemented to promote or punish a driver's behavior?

For connected vehicles to monitor drivers, there will be some form of technology collecting data while a driver is in the car's interior. The interior of the car is considered a place with a reasonable expectation of privacy even under the Fourth

Amendment of the U.S. Constitution. *New York v. Class*, 475 U.S. 106, 114-115 (1986). And studies show that drivers and passengers are not comfortable with car systems monitoring them while they are in the car.

With the development of personal privacy laws on a global scale, if the interior of the car is monitored, a notice of data collection to the drivers and passengers will be needed. For example, a video recording of the interior will likely collect racial or ethnic information because it will record the likeness of the driver and the passengers. If the vehicle monitors the speed limit of the road, precise geolocation is also likely to be collected to determine the speed limit of the road. These categories of information are considered sensitive information under the California Privacy Rights Act (CPRA) and the General Data Protection Regulation (GDPR) of the EU. See Cal. Civ. Code § 1798.140(ae)(1)(A)–(F); see also 2016 O.J. L 119/1 §9(1).

The CPRA gives a California consumer the right to limit the use of sensitive personal information to that which is necessary to perform the services or provide the goods reasonably expected by an average consumer. Cal. Civ. Code § 1798. 121(a). Likewise, GDPR requires explicit consent to process sensitive personal information. 2016 O.J. L 119/1 §9(2). Drivers are likely to opt out of the collection in the U.S. and not consent to data collection while driving.

Car companies and manufacturers may try to justify the collecting, using, and processing sensitive personal data based on the legal obligation to comply with traffic laws. However, one could argue that collecting sensitive information to allow someone to drive is unnecessary and not something consumers reasonably expect because drivers do not provide that data to drive today.

Moreover, the collected data may be misinterpreted by the algorithm. Suppose the vehicle monitors the driver's behavior to identify drunk driving and stops the vehicle after recognizing a drunk behavior. If it is later determined that the driver had diabetes with low blood sugar that made him/her appear drunk, the data collected may suddenly become medical information, and the purpose of the collection may be challenged by the driver.

One answer to avoid misinterpreted data collection may be to implement a combination of data collection systems. Using the infrastructure law as an example, the car may be equipped with a breathalyzer and a video monitoring system to assure that the data collection is for drunk driving. This could reduce the chance that the driver's behavior is caused by something other than alcohol. However, the facts may become even more complicated if a passive breathalyzer picks up the alcohol content from the passenger instead of the driver. New technology and ideas may provide a safe harbor to justify collecting and using sensitive data. These new methods still cannot resolve the question of whether consumers will be comfortable and accept the monitoring of their driving behavior in the interior of the car, especially when the monitoring could potentially limit the driver's ability to drive freely.

Should Connected Vehicles Make Driving Decisions for Drivers?

GDPR sets forth that data subjects have the right not to be subject to automated decision-making, including profiling. 2016 O.J. L 119/1 §22(1). Evaluating data to determine a driver's right to operate a vehicle without human intervention would most likely violate the GDPR. As part of safeguarding the data subject's rights and freedoms, the GDPR provides the data subject with the right to obtain human intervention to contest the automatic decision making. 2016 O.J. L 119/1 §22(3).

The CPRA instructs the California Attorney General to issue regulations for consumers to opt out from a businesses' use of automated decision-making technology. Cal. Civ. Code § 1798.185(16). Implementing technologies like prohibiting drunk driving or throttling speeding based on the connected car's algorithm would likely conflict with the privacy laws and regulations in the U.S. At least under the CPRA, any form of social credit, or in this case a driving score, could be considered "profiling" because the collected data would be used to evaluate personal aspects of a person to predict the reliability and behavior of the driver whose information is being processed.

In connected cars, there is no reasonable or effective way to contest the car's decision to prohibit a driver from driving for reasons of drunk driving or stopping the car from throttling the speed limit. Drivers' right to drive is affected when the algorithm makes the decision. OEMs and first-tier suppliers should be aware that data processing that results in an automated response by the connected car may be subject to the growing concerns of privacy laws not just in the U.S. but around the world.

Conclusion

There is no doubt that connected cars will be the next "device" that will provide consumers with added safety and convenience through using big data. As more data is collected, there will be a push to use the data for better traffic safety and optimal driving experiences. But the automotive industry will have to strike a delicate balance between safety through data processing and privacy.