SCHOLARS
STRATEGY NETWORK

The Unintended Consequences of New Regulation on Advanced Impaired Driving Technology

Zahid Anwar, North Dakota State University
Zia Muhammad, North Dakota State University

There were 42,915 fatal traffic crashes in the United States in 2021 alone, a 10.5% increase from 38,824 fatal crashes in 2020. Among these fatalities, 30% of accidents occurred in which at least one driver was drunk or alcohol-impaired. These statistics are not surprising as drunken driving affects drivers in several ways, including but not limited to blurred vision, inhibited judgment, behavioral changes, dizziness, and impaired reflexes. Being one of the leading causes of fatal crashes in the U.S., drunken driving is, therefore, a serious threat to the life of drivers, passengers, and pedestrians.

In order to address this public safety crisis, the 117th Congress included SEC. 24220 in its $1 trillion infrastructure plan. The legislation forces the automotive industry to roll out advanced impaired driving technology like alcohol detection sensors in all new vehicles as early as 2026.

Although Congress's new law is a great start, there is still a long way to go to ensure the development of cyber-secure, accurate, and tamper-proof hardware in vehicles.

The Technology

According to the National Transportation Safety Board, automakers can detect impaired drivers using a combination of integrated alcohol detection systems, driver monitoring cameras, and advanced driving monitoring systems. The National Highway Traffic Safety Administration funded $55 million for the development of the Driver Alcohol Detection System for Safety (DADSS) program. This program is broadly classified into two categories (1) the breath system that uses infrared light to detect the presence of alcohol to carbon ratio, and (2) the touch system embedded in the ignition button that uses near-infrared tissue spectroscopy to read alcohol levels below the skin.

The Driver Alcohol Detection System for Safety is predicted to be able to detect alcohol concentration within 0.8 seconds. If a driver is detected to be impaired at the start of the driving session, the system is designed so as to disable the vehicle from starting. On the other hand, if someone is not drunk to begin with but becomes impaired during the drive, then the sensors will still be able to detect that change due to a passive monitoring system. In this case, the car will turn on hazard lights, make beeping sounds, deaccelerate, and even pull over to the side of the road off to the shoulder.

Although this technological innovation is certainly promising in its ability to save lives, reduce injuries, and encourage a healthy lifestyle, it also raises some questions regarding trust and privacy.

Issues with Data Collection and Cybersecurity

There may be uncontrolled data collection for drivers, whether they are drunk or not. The manufacturers can utilize deployed sensors in combination with other vehicular sensors like GPS and cameras to track a vehicle's location, preferences, and monitor activities of daily living. For example, the manufacturer would be able to trace routine patterns such as fueling, shopping, and dining.

Sensors may be vulnerable to cybersecurity threats as they communicate with vehicles using different communication protocols. These sensors also use embedded software to interpret results—and whenever there is software involved, there are vulnerabilities. Successful exploitation of vulnerabilities leads to cyberattacks. In the past, multiple vulnerabilities were found in sensors, and many vehicles were hacked.

Selling vehicle data may become a business, and the potential buyers can be car insurance agencies, automakers, high-tech firms, and third-party advertising companies. Although the users' data is collected for business intelligence, interest-based advertisements, and to enhance users' experience, it may also be sold for financial benefits, therefore, making it an ideal target for hackers.

Deliberate Misuse of Sensors

An additional issue is the possibility of tampering with safety hardware to deceive the sensor's detection system into starting the vehicle even if the driver is drunk. In the past, there have been cases recorded where end users tampered with mileage gauges and vehicle engine lights. Likewise, GPS "spoofing" is also very popular in the car rental and automotive industry for stealing and hiding vehicles. Similar techniques can be used on drunken sensors for personal advantage.

Sensors may also be deceived using simple tricks like breath analyzers can be deceived if a person drives a vehicle with open windows or an open sunroof. Similarly, the use of face masks like N95 can trap air molecules and partially interfere with the detection capability of sensors. Meanwhile, touch-based alcohol sensors can also be affected by the use of infrared protection gloves.

Insurance and the New Car Market

Insurance prices may increase in certain cases where a person is routinely drunk and attempts to start a vehicle. Since every attempt can be monitored, logged, and collected by automakers, they can further share this information with law enforcement and insurance agencies if required.

A drop in the market of sensory vehicles can be expected, as buyers may be weary of this new technology. Therefore, there is a possibility that people will prefer to buy vehicles without these sensors. Even if the regulation mandates all automotive manufacturers install sensors, many people may prefer to own old vehicles that do not have sensors instead of buying new ones.

Recommendations

This technology has tremendous potential; however, the deployment must be justified with research and development of cyber-secure, accurate, and tampering-proof hardware. Likewise, the National Highway Traffic Safety Administration must provide minimum base guidelines for the design of safe sensors and must define a threshold of data collection and third-party disclosure. Otherwise, uncontrolled data collection, user tracing, cyber threats, and data breaches may be unavoidable.