



March 19, 2015

Jean Shiomoto
Director
Department of Motor Vehicles
2415 1st Ave., Mail Station F101
Sacramento, CA 95818-2606

Re: "Autonomous Vehicle" Regulations

Dear Director Shiomoto:

I am writing on behalf of Consumer Watchdog to express our concern that Google and others with a vested interest in developing "autonomous vehicle technology," also known as driverless cars, are pushing the Department of Motor Vehicles into promulgating rules regulating the public use of these vehicles on California's highways that are inadequate to protect our safety. Safety issues are paramount, of course, but there are other substantial questions about privacy, data security and insurance that are also raised by driverless cars. The DMV regulations now being written governing the public use of autonomous vehicles should reflect these important questions as well.

Safety issues: Despite Google's public relations campaign suggesting that a robot or driverless car is just around the corner, there is no doubt that it will be many decades before a fully automated vehicle system replaces the personal responsibility model, based on a driver at the wheel, that has governed our transportation system since the advent of the mass production automobile.

The DMV promulgated regulations that went into effect Sept. 16, 2014 governing the testing of driverless cars on California highways. One of the key and necessary safety provisions of the testing regulations is the requirement that there must be a test driver in the driver's seat who is capable of assuming control of the car if there is a problem. Ironically, a little more than a week after the DMV adopted the testing regulations, Google announced plans for a fleet of robot cars that have no steering wheel, brake pedal or accelerator. In Google's fleet there would be no way for an occupant to take control in an emergency; occupant lives would be in the hands of Google's driverless technology, completely at the Internet giant's mercy.

Despite Google's public relations campaign and statements that it hopes to have robot cars for public use operating on the road within five years, it is important to understand what its vehicles cannot do. Recognition of the Google driverless cars' shortcomings should help inform the DMV's "autonomous vehicle" public use rulemaking process.

Google's robot cars rely upon meticulously gathered information about the roads they travel. This detailed data is gathered by human-driven scanner cars and is far more detailed

than what is provided on Google Maps. So, while Google says its driverless vehicles have navigated more than 700,000 miles without incident, it's 700,000 miles on only a few specially mapped and analyzed routes. If a Google driverless car tried a route that had not been specially mapped, probably even a large parking lot, the car wouldn't know what to do.

One bit of information gleaned from the detailed mapping and route analysis is when a car should expect a traffic light. However, if the sun is behind the traffic light, it can interfere with the driverless car's video sensors and the car's ability to determine the traffic light's color. Or, if the light were installed overnight as in the case of a road construction site, the car's driverless navigation system would not expect it. Also problematic would be a situation where a traffic light was expected, but was not functioning, perhaps because of a power outage.

The cars don't perform well in bad weather. Because heavy precipitation interferes with the vehicle's video sensors, they don't work in the snow, nor in heavy rain. The sensors don't recognize large potholes and worse, would not detect an open manhole. The cars' sensors apparently can recognize a stop sign and the car would react properly if a construction worker held one up. A policeman, however, using only hand signals to direct traffic, would likely be ignored. Indeed, the driverless cars' video sensors can't reliably distinguish between a tree branch blowing in the wind and a pedestrian.

Perhaps in the distant future when there are many driverless cars on the road the vehicles will have the technology to communicate with each other, helping them navigate through traffic. Currently, however, there would be few such vehicles and in most cases the robot cars would be interacting with cars driven by humans. Frequently, say at a four-way stop intersection, drivers communicate their intentions with hand signals or even a nod of the head. How could a driverless car interact in a safe and meaningful way with a human driver in another vehicle in such a situation? It couldn't.

In short, California is a long, long way from the so-called "autonomous vehicle." Instead, most objective observers expect a step-by-step progression to greater automation of vehicle functions – but with the driver always required ultimately to be in control. As exciting as the prospect of improved automated safety technologies may be, experience suggests their development and application will take many years – and that there may be finite limits to the degree of automation that will be acceptable.

Completely driverless cars with no provision for a human takeover when the autonomous technology fails or is inadequate to cope with a given situation should be banned from California's highways unless, and until, every car with a driver is replaced by one with just a computer. As outlined above there are clear circumstances when existing driverless technology alone is inadequate for a vehicle to operate safely. An essential provision in the rules now being developed governing the public use of autonomous vehicles should be the requirement that a licensed driver must be capable of taking over operation of a driverless car whenever necessary.

Privacy and Security Concerns: Internet technology was implemented with little regard to protecting users' privacy. We are playing catch-up for our failure to consider the societal impact of a new technology. The time to ensure that this new driverless car technology has the necessary privacy protections is while it is being designed and developed. This is a concept known as "Privacy by Design." It means privacy issues are considered from the very beginning and solutions are "baked in." Trying to catch up after a new technology is developed and broadly implemented simply will not work.

Google was the driving force behind SB 1298, which charged the DMV with the task of developing the regulations and also rebuffed attempts to deal with consumer privacy. The DMV regulations now being written must give the user control over what data is gathered and how the information will be used. Merely stating what data is gathered with no explanation of its use is woefully inadequate. The DMV's autonomous vehicle regulations should provide that driverless cars gather only the data necessary to operate the vehicle and retain that data only as long as necessary for the vehicle's operation. The regulations should provide that the data must not be used for any additional purpose such as marketing or advertising without the consumer's explicit opt-in consent. Finally, DMV regulations should require that the data gathered by a driverless car is adequately encrypted and securely stored.

Without appropriate restrictions, autonomous vehicles will be able to gather unprecedented amounts of information about the use of those vehicles. Just as we are now tracked around the Internet, will Google and other purveyors of driverless car technology now be looking over our shoulders on every highway and byway? Will the data be provided to insurance companies for underwriting purposes or to third parties that develop some kind of a driving score related to where and when individuals travel? Will it be used to serve in-car advertisements or advertisements through other venues in the Google suite of products? Will it be used to track our movements and those of surrounding cars and mobile devices so that Google's advertisers can better locate us?

Personal security is closely related to privacy. Tomorrow's motorists will face the threat that hackers will be able to assume control of their vehicles. Privacy and security must be hard-wired into automated technologies from the outset. Unfortunately, as the massive data breaches of recent years have demonstrated, there is little financial incentive to undertake the expensive hardening of technologies absent significant statutory liability for the failure of hardware and software manufacturers to prevent third-party data incursions. If anything, technology is increasingly deployed against the consumer. Lending institutions, for example, are adding remote kill switches to cars, enabling banks to disable the vehicle if a loan payment is overdue. Now is the time to establish the privacy and security parameters that will guide data and security protections in the future.

Insurance issues: Although insurance issues will remain primarily the responsibility of the California Department of Insurance, the DMV should be cognizant of the fact that some of your decisions – such as requiring a human driver be able to take control – will impact insurance issues.

So long as consumers are personally responsible for maintaining and operating their vehicles in order to prevent accidents, the Proposition 103 insurance reforms enacted by California voters will be necessary to protect consumers. Proposition 103 was enacted by the voters twenty-six years ago to both hold rates to fair levels and ensure that each motorist's premium is based on rating factors within their control – principally their driving safety record, the number of miles they drive annually, and years of driving experience, along with optional rating factors adopted by the Commissioner regulation that are “substantially related to the risk of loss.” (Ins. Code section 1861.02.)

Under any system in which a motorist is or may be responsible for controlling the vehicle, the motorist's individual responsibility, as reflected by their driving record, will remain of paramount importance, and thus the single most important determinant of their premium, as the statute specifies. Similarly, annual mileage and years of driving experience reflect the motorist's risk, whether or not the policyholder is driving a car that is equipped with automation technology. Cars equipped with improved technology will be rated, as they are today under Proposition 103, based on their repair or replacement cost for purposes of comprehensive (weather damage, fire and theft) and collision coverages.

Just as it is today under our product liability laws, responsibility for an accident will be allocated to manufacturers of hardware or software whose product was responsible for an accident or injuries.

Vehicle Certification: The decision on whether to allow a particular manufacturer's driverless cars to be offered for public use should be informed by the results of safety testing that is being done under the DMV testing regulations that are now in effect.

Under these regulations a manufacturer must file reports explaining when and why a test driver had to take over operation of the car and details of any accidents. The first such testing reports would cover the period from when a test vehicle received a permit – presumably Sept. 16, 2014 – through Nov. 30, 2015. These reports would be due by Jan. 1, 2016.

Consumer Watchdog believes that no public use of an “autonomous vehicle” should be allowed until the results of at least a year's tests are available and subject to public scrutiny. The incident reports are due Jan. 1, 2016, but sufficient time – a minimum of six months – must be allowed to analyze the test results. Consumer Watchdog urges the Department to include a requirement in the public use rules for a year of testing under DMV regulation and six months to analyze the test data before a driverless car could be offered to the public, with extensions as necessary if the test data uncovers safety problems. Under the rules we are proposing, the earliest time a “driverless car” could be approved for public use on California's highways would be July 1, 2016. It would require a licensed driver who could take over when necessary.

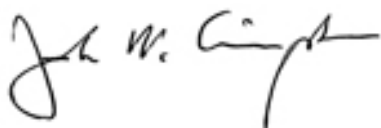
Consumer Watchdog strongly supports the development of new automotive technologies, particularly those that will prevent deaths and injuries (and reduce dependence on fossil fuels). Many of the technologies under development today could, if affordable

enough to be widely deployed, reduce accidents and ultimately lower auto insurance premiums.

It is possible, perhaps even likely, that the technology needed to manufacture vehicles that operate “autonomously” with one hundred percent safety will eventually be perfected. In the meantime, under any realistic scenario for the near or even distant future, human drivers will be responsible for maintaining control of their vehicle in order to prevent an accident.

We call on the DMV to ensure the public interest is put ahead of the self-serving agendas of the autonomous vehicle technology manufacturers. Regulations to protect data privacy and security must be put in place. The autonomous vehicle regulations for public use should require a full year’s results of testing under DMV regulations with at least six months to publicly scrutinize and analyze the results before a vehicle can be certified for public use. Most importantly, a driverless vehicle must allow a licensed driver to assume control when necessary.

Sincerely,

A handwritten signature in black ink, appearing to read "John M. Simpson". The signature is fluid and cursive, with a prominent initial "J" and a long, sweeping underline.

John M. Simpson
Privacy Project Director

Cc: Brian G. Soublet, Randi Calkins