



DMV's Autonomous Vehicle Regulations Must Protect Users' Privacy
-- John M. Simpson, Privacy Project Director, March 11, 2014

I am speaking on behalf of Consumer Watchdog, nonpartisan, nonprofit public interest group, to call on the Department of Motor Vehicles to ensure that the regulations you are developing to govern the use of autonomous vehicles – popularly known as driverless cars – will protect the operators' privacy.

The company most directly affected by the new autonomous vehicle regulations will be Google, which is pioneering development of the robot-driven cars. The Internet giant was the driving force behind SB 1298, which charged the DMV with the task of developing the regulations and also rebuffed attempts to require privacy protections in the law.

However, it is not too late to implement privacy safeguards in this rulemaking and Consumer Watchdog calls on the DMV to do so. Failure to act will mean substantial privacy risks from the manufacturers' driverless car technology if there are not protections from what Google is best known for: the collection and use of voluminous personal information about us and our movements.

The DMV regulations 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 must 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.

Without appropriate regulations, autonomous vehicles will be able to gather unprecedented amounts of information about the use of those vehicles. How will it be used? 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?

As I mentioned, Google is leading driverless car research and is attempting to steer regulatory efforts in various states, especially California. That's why my comments are so focused on the company. So I ask: Why won't Google endorse simple privacy safeguards for its self-driving cars? I think there are two reasons.

First, Google's entire business model is based on building digital dossiers about our personal behavior and using them to sell the most personal advertising to us. You're not Google's customer; you are its product – the one it sells to corporations willing to pay any price to reach you. Will the driverless technology be just about getting us from point to point or more about tracking how we got there and what we did along the way?

Second, computer engineers, who believe that more data is always better, are in charge at Google. They may not know what they would use data for today, but they think they may someday find a use for it and don't want any restrictions on them now.

Google is first and foremost an advertising company; 98 percent of its \$38 billion in revenue comes from advertising, and the more personalized the marketing the better. Indeed, Executive Chairman Eric Schmidt has said, "We don't need you to type at all. We know where you are. We know where you've been. We can more or less know what you're thinking about."

You may remember the last time Google deployed high tech vehicles around the world. The result was Wi-Spy, the biggest wire-tapping scandal in history when the company's Street View cars sucked up data from tens of millions of private Wi-Fi networks, including emails, health information, banking information, passwords and other data. The company paid \$7 million to settle the case brought by the state attorneys general. A class action suit is pending in federal district court.

Citing its "Don't Be Evil" motto, Google claims it can be trusted with our information. Facts show otherwise. The FCC released documents showing the Wi-Spy scandal was not a mistake or the work of one rogue engineer, as the company had claimed; but was part of the Street View design. The Commission fined Google \$25,000 for obstructing its investigation.

The Federal Trade Commission imposed a \$22.5 million penalty on Google for violating a consent agreement and hacking around privacy settings on Apple's Safari browser, which is used on iPads and iPhones. Simply put, there is no reason to believe Google when it claims to be concerned about privacy.

Consumers enthusiastically adopted the new technology of the Internet. What we were not told was that our use of the Information Superhighway would be monitored and tracked in order to personalize corporate marketing and make a fortune for companies like Google. Consumer Watchdog supports driverless car technology and predicts it will be commonplace sooner than many of us expect. However, it must not be allowed to become yet another way to track us in our daily lives.

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. I call on the DMV to require that consumers must give opt-in consent before any data gathered through driverless car technology is used for any purpose other than driving the vehicle.

While we don't propose to limit the ability of the cars to function by communicating as necessary with satellites and other devices, the collection and retention of data for marketing and other purposes should be banned. Unless strong protections are enacted in the new regulations, once again society will be forced to play catch-up in dealing with the impact of the privacy invading aspects of a new technology.

#####