LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
TUESDAY, FEBRUARY 13, 2018

The future of privacy

By Jonathan Michaels

Shutterstock

It all started with Cadillac really. In 1996, General Motors introduced the Cadillac OnStar system — an onboard communication system that linked active drivers with a GM call center — and with that the world of consumer privacy forever be changed. The OnStar system was a road paved with the best of intentions. Drivers could get hands-free, turn-by-turn directions or call for dinner reservations, and in the event the vehicle's airbags deployed, the call center would automatically dispatch emergency units.

Yet with the development of this technology a national debate ensued, which has now been two decades in the making. What started out as seemingly benign has turned into anything but, as analog motoring steps aside in favor of the digital era. Connectivity was initially defined as unobtrusive baseline communication between motorists and call centers. Now, however, connected cars often know more about drivers than their spouses, as every movement, every stop is digitally recorded.

To put the issue in perspective, consider that the first space shuttle contained some 500,000 lines of software code. Today, the average 2018 automobile contains 100 million lines, all of which are working together to transmit information to the automakers who created them. At present, 78 million cars are embedded with a cyber connection. By 2021, technology research firm Gartner estimates that 98 percent of all cars will connected. Like to stop by Starbucks at 8:15 every morning? Your car will know it — and so will its manufacturer.

And therein lies the issue. To whom does this private information belong? Presently, no U.S. laws govern the ownership, storage or use of data collected on motorists' behavior. In 2014, 19 automakers issued a pledge to the U.S. Department of Transportation, promising self-governance on how private motoring data collected would be used. Under the Privacy Principles for Vehicle Technologies and Services, manufacturers promised to restrain from selling motorist data to third-parties absent consumer consent. What the pledge doesn't reveal, however, is that most manufacturers request and obtain that consumer consent in fine print buried deep in purchase agreements, leading to a real lack of appreciation as to the digital relationship that exists.

If there is any question on how this information is being harvested and used, Israeli startup company Otonomo seems to provide the answer. The self-proclaimed "first connected car data marketplace," Otonomo has been leading the charge to monetize motorist data. Currently, nine car manufacturers give Otonomo access to their raw data, who then analyzes its, packages it and sells it to third parties, sharing the profits with the automakers.

And don't expect this business model to slow. Automotive giant and parts supplier Delphi recently invested $25 million in Otonomo, hoping to capitalize on the wideopen market selling consumer data for substantial profit. To be sure, it is not lost on automakers that selling consumer data is 100 percent margin, while turning new cars is a still single-digit margin game.

Exactly how invasive will the practice be? Motoring data will allow manufacturers to create a behavior fingerprint of sorts on each consumer, giving merchants the ability to market to individual consumers with known behavior. Make a trip to Taco Bell every week? Don't be surprised to see your inbox fill up with advertisements from south of the boarder.

While the peddling of some behavioral data might register as merely annoying, one could imagine a host of scenarios that invade much further. For instance, what of the motorist who secretly makes a trip to the HIV clinic each week, expecting his health concerns to be known only to him? The clinic is bound to secrecy by the federal privacy rule known as HIPAA, but collected motoring data is free to be sold to the highest bidder. Or how about consumer data that could be sold to insurance companies, who will know now exactly how often you speed, how frequently you wear your seatbelt, and how far you drive every day. At best, the leakage of such private information could be galling; at worst, the selling of personal behavioral data could be seriously disruptive, or even life-altering.

And then there is the matter of security. According to the book

"Code Complete" by software expert Steve McConnell, the best software companies can push programing errors down to about 0.5 bugs per 1,000 lines of code. If true, this means that the typical new automobile has approximately 50,000 bugs, raising the question of how secure is data, and what happens in the event of a breach? Students of history will remember the 2015 recall of 1.4 million Jeep vehicles, after white-hat hackers demonstrated that they could take over operation of a Jeep Cherokee from a laptop located some distance away.

Privacy concerns in the automotive sector are nothing new, and in fact legislation has been enacted to address other areas of confidentiality. The Driver's Privacy Protection Act of 1994 regulates the disclosure of personal information contained in the records of state motor vehicle departments, while the similarly named Driver Privacy Act of 2015 covers ownership of data recorded by monitoring devices, such as a vehicle's event data recorder.

There is hope that an answer will soon evolve. This past June, the Federal Trade Commission and the National Highway Traffic Safety Administration hosted a workshop on the issues of privacy and security in connected cars. Yet as with most technology issues, the advancement of computing expertise far outstrips the evolution of appropriate legislation.

Without question, the technology present in connected cars is not just convenient, it presents an enormous overall societal good. A 2015 study commissioned by the global management firm Boston Consulting Group revealed that driver assisted technology can help avoid 28 percent of all of today's automobile accidents, preventing approximately 9,000 fatalities per year, and saving $250 billion in societal costs annually.

The answer to the riddle is not to quell automotive advancement, but to harness it in a way that can allow its powerful benefits to be employed, while maintaining a reasonable level of confidentiality in the data harvested. We are close, but until federal regulation controls profiteering manufacturers, we will all be at risk of having our every move monetized on the open market.

Jonathan Michaels *is the founding member of MLG Automotive Law, APLC, which specializes in representing clients in the automotive industry. You can reach him at (949) 581-6900 or jmichaels@mlgautomotivelaw.com*