Cars and Privacy by Michael Whitener

Smart cars are invading the roadways. These "computers on wheels" are equipped with everything from global positioning systems to WiFi, electronic data recorders and trackers to record driving habits for insurance companies. In-car technology is advancing at an incredible rate. Self-driving cars that once only existed in science fiction novels are now a reality, and cars can give drivers real-time feedback on their driving performance through cameras and data recorders.

These new automotive technologies offer improved safety, navigation, diagnostics, entertainment and other advantages – but what do they mean for our privacy and data security?

It's useful to think of connected cars in three distinct contexts:

- **On-board diagnostics (OBD) and event data recorders (EDR).** These computer systems have been on cars since the late '90s and require physical access to the vehicle. No particular privacy/security issues here.
- **"Fitbit" style tools like those offered by the company Automatic.** These are essentially extensions of your mobile phone. Privacy issues can be addressed as with other mobile apps.
- **New wireless technologies.** These are the types of technologies – like those in the Tesla Model S – that have people worried.

There are no US laws that explicitly regulate the collection of auto data. The Federal Trade Commission, in its recent "Internet of Things" report, decided not to recommend legislation aimed at connected cars and other devices, but instead is advocating broad-based, technology-neutral data security and privacy legislation.

The auto industry has come out with proposed Privacy Principles for connected cars (beginning with model year 2017), but Senator Markey (D-Mass) – in a report his staff issued in February – found fault with them. According to the Markey report, Tracking & Hacking: Security & Privacy Gap Puts American Drivers at Risk, there is a "clear lack of appropriate security measures to protect drivers against hackers who may be able to take control of a vehicle or against those who may wish to collect and use personal driver information." The report also noted that automakers collect and utilize large amounts of driving data, and the majority transmit that data to third parties.

The Markey report has led to calls for mandatory standards to protect drivers' data, security and privacy. The challenge will be to ensure that privacy and data security principles are satisfied while also encouraging technological innovation by automakers and their suppliers.

Michael Whitener is a VLP Partner. Michael conducts privacy audits and risk assessments, drafts privacy policies and data transfer agreements, and advises on compliance with U.S. and foreign data privacy laws and regulations, including COPPA, HIPAA, the Gramm-Leach-Bliley Act and the EU Data Protection Directive (e.g., Safe Harbor certification).