Navigating the Data Privacy Landscape for Autonomous and Connected Vehicles: Implementing Effective Data Security

Article By

Adam J. Brody
John J. Rolecki
Jeffrey M. Stefan II
Andrea M. Gumushian
Justin M. Wolber

Varnum LLP
Advisory

Related Practices & Jurisdictions

- Communications, Media & Internet
- Utilities & Transport
- All Federal

Wednesday, May 18, 2022

Autonomous vehicles can be vulnerable to cyber attacks, including those with malicious intent. Identifying an appropriate framework with policies and procedures will help mitigate the risk of a potential attack.

The National Highway Traffic Safety Administration (NHTSA) recommends a layered approach to reduce the likelihood of an attack’s success and mitigate ramifications if one does occur. NHTSA’s Cybersecurity Framework is structured around the five principles of identify, protect, detect, respond and recover, and can be used as a
basis for developing comprehensive data security policies.

NHTSA goes on to describe how this approach “at the vehicle level” includes:

- **Protective/Preventive Measures and Techniques**: These measures, such as isolation of safety-critical control systems networks or encryption, implement hardware and software solutions that lower the likelihood of a successful hack and diminish the potential impact of a successful hack.

- **Real-time Intrusion (Hacking) Detection Measures**: These measures continually monitor signatures of potential intrusions in the electronic system architecture.

- **Real-time Response Methods**: These measures mitigate the potential adverse effects of a successful hack, preserving the driver’s ability to control the vehicle.

- **Assessment of Solutions**: This [analysis] involves methods such as information sharing and analysis of a hack by affected parties, development of a fix, and dissemination of the fix to all relevant stakeholders (such as through an ISAC). This layer ensures that once a potential vulnerability or a hacking technique is identified, information about the issue and potential solutions are quickly shared with other stakeholders.

Other industry associations are also weighing in on best practices, including the Automotive Information Sharing and Analysis Center’s (Auto-ISAC) [seven Key Cybersecurity Functions](https://www.natlawreview.com/article/navigating-data-privacy-landscape-autonomous-and-connected-vehicles-implementing) and, from a technology development perspective, SAE International’s J3061, a [Cybersecurity Guidebook for Cyber-Physical Vehicle Systems](https://www.natlawreview.com/article/navigating-data-privacy-landscape-autonomous-and-connected-vehicles-implementing) to help AV companies “[minimize] the exploitation of vulnerabilities that can lead to losses, such as financial, operational, privacy, and safety.”

© 2022 Varnum LLP

National Law Review, Volume XII, Number 138