Eight Tips to Prevent Autonomous Vehicle Cyber Breach Liability

Insights
8.16.18

The autonomous vehicle revolution promises many benefits. To name a few: eliminating virtually all accidents; drastically reducing traffic congestion; and providing an economical and environmentally friendly mode of transportation. However, if AVs are to achieve their full potential, interconnectivity is the key. AVs will need to communicate with each other, the surrounding infrastructure, and with a host of platforms.

Interconnectivity is not possible without software, and AVs will feature millions of lines of code. This means cyber security is a chief concern, and numerous articles have been written addressing the abundant threats and how to combat them. This article is not one of them.

Instead, this article addresses how companies in the AV industry can best position themselves to avoid liability for a cyber breach. The reality is that no matter how many steps are taken to prevent a breach, the threat cannot be entirely eliminated. Even if every reasonable step is taken, malicious hacking or user negligence remain a threat. And even if you take every imaginable precaution to avoid a breach, inevitably one will happen, and some lawyer, somewhere, will be willing to represent the victims of that breach. You can also bet that same lawyer will sue anyone and everyone arguably connected to the incident. This includes vehicle owners, OEMs, software manufacturers.

Here are eight tips to avoid AV cyber breach liability:

1. **Identify information vulnerable to a breach** – What information is vulnerable if something goes wrong with respect to your product? Is it information shared with the vehicle through a user's smart phone? Is it metropolitan traffic pattern information? Is it information through which a hacker can take control of a vehicle? Identifying the information at risk is a necessary precursor to the steps outlined below.
2. **Prepare a written breach incident response plan** – The worst time to figure out how to respond to a breach is after one has occurred. Think through the possibilities in advance. Create and identify members of a breach response team. Decide who is going to do what, when and how. Retaining outside attorneys to help design and implement plans can help preserve attorney-client privilege. And don't forget requirements imposed by breach notification statutes. These laws, which exist in almost every state, frequently impose stringent consumer notification

requirements. The time to decipher these statutes and determine requirements is before a breach, not after.

3. **Identify and comply with applicable statutory and regulatory requirements** – Compared to other industries, the AV industry is relatively unregulated. The regulatory focus to date has largely centered on testing AVs and providing broad brush guidelines for their development. Because AVs embrace new and emerging technologies, the applicable legal landscape undoubtedly will shift. Yet, when it comes to data privacy and cyber security, there are existing domestic and international statutes, regulations and legal principles that industry players should take into consideration. For example, companies should consider the "privacy by design" approach endorsed by the FTC. Under that approach, companies are encouraged to build security into their devices early in the development stage, rather than as an afterthought. To this end, manufacturers and designers should consider conducting a privacy or security risk assessment, minimizing the data they collect and retain, and testing their security measures before launching their products.
4. **Communicate across the supply chain continuum** – Extremely few companies, if any, are situated to design and manufacture AVs from start to finish. Development of AVs will require contributions from software manufacturers, OEMs, and vehicle manufacturers alike. Communication between suppliers, contractors, and others is essential to understand and agree upon intended usage, integration, and requirements. Specifying rights and obligations in writing is key. Today's suppliers have greater leverage to shape contract verbiage than they have had in the past. This is because emerging technologies are not as widely available as other vehicle components have been in the past, and manufacturers therefore have fewer options.
5. **Utilize outside counsel** – Although this advice sounds self-serving given the identity of the author, the aftermath of a data breach is no time to go it alone. AVs promise to bring previously unimagined conveniences to passengers, but to do so, AVs will accumulate extensive consumer data. The number of contributors across the supply chain continuum make it all the more likely that it will be difficult to determine who is required to do what in the event of a breach. Does the obligation to notify consumers fall on the vehicle manufacturer, the OEMs, the software manufacturer, municipalities who provided malfunctioning infrastructure, or all of them? Given the rollout of such vehicles in interstate commerce and the diverse geographic consumer footprint, what state laws apply? What must be done in the event of a breach and when? Waiting for litigation to retain outside counsel is a poor decision. Counsel can help you identify steps that are not only suitable under the circumstances, but that will aid in avoiding or minimizing liability should litigation ensue.
6. **Don't waste time** – When a breach occurs, it is hard to figure out what happened and how it happened. It can be tempting to try to "get all the answers" before taking action, but delays can sometimes run afoul of time requirements under breach notification statutes. Data breaches are not like wine; they don't get better with age.
7. **Train your employees** – Preparing policies, drafting appropriate contracts, and understanding your obligations are only helpful if your employees understand why you are taking these steps

and for what purpose. Explain your policies to your employees and periodically train them. Assess your employees under training and work to improve their performance.

8. **Consider purchasing cyber liability insurance** – CGL policies can cover damage to tangible property, but they likely will not provide protection for the significant legal costs that can arise in the event of a cyber breach. Checking with your insurance broker to understand the extent of protection in place is a wise move.

This is an exciting time in human history. The emergence of new technologies is changing the world in beneficial and unexpected ways. Cyber security is an imperfect science. Mistakes will be made, and accidents will happen. Identifying who is legally responsible will be determined in part by yet-to-be enacted laws and regulations, and in part by decisions in the courtroom. As with any legal dispute, parties who behave reasonably and prudently prior to an incident will fare better. Take some time to consider how you would fare and whether there is more you should be doing now.

If you have questions or concerns regarding how companies in the AV industry can best position themselves to avoid liability for a cyber breach, contact Mike Greco or any member of our Autonomous Vehicles Practice Group.

This article was originally published by *Automotive IQ* in May 2018.

Related People

Michael R. Greco
Regional Managing Partner
303.218.3655
Email