REPRINT

CD corporate disputes

HIGHLY AUTOMATED AND CONNECTED VEHICLES: DATA PRIVACY AND THIRD-PARTY LIABILITY

REPRINTED FROM:
CORPORATE DISPUTES MAGAZINE
OCT-DEC 2020 ISSUE

www.corporatedisputesmagazine.com

Visit the website to request
a free copy of the full e-magazine

SHOOK
HARDY & BACON

Published by Financier Worldwide Ltd
corporatedisputes@financierworldwide.com

www.corporatedisputesmagazine.com

ONE-ON-ONE INTERVIEW

HIGHLY AUTOMATED AND CONNECTED VEHICLES: DATA PRIVACY AND THIRD-PARTY LIABILITY

Tatiana Rice
Associate
Shook, Hardy & Bacon L.L.P.
T: +1 (202) 783 8400
E: trice@shb.com

Tatiana Rice's practice focuses on solving complex issues related to technology and electronically stored information for clients. Her focus is on pre-trial litigation strategies, data privacy, and government investigations and compliance.

CD: Could you provide an overview of recent developments in the highly automated and connected vehicles field? How would you describe their evolution?

Rice: One interesting and obvious development is the variety of use cases for highly autonomous vehicles (HAVs) in the age of COVID-19. With more pressure for companies to conduct contactless services, such as delivery, consumers are seeing value in HAVs in ways that were not obvious before. For example, Nuro, a Silicon Valley-based autonomous vehicle start-up launched in 2016, has grown 300 percent as large businesses, including Walmart, Kroger and Domino's Pizza, are using their HAVs to conduct contactless deliveries and reduce risk of spread. It appears that Nuro has also recently partnered with CVS to conduct contactless prescription deliveries. Of course, much of this progress is still in the testing phase, but it is just another example of how challenges our society faces can be solved through technological innovation. On the other hand, however, the pandemic has also halted a lot of momentum for other autonomous vehicle projects, such as shared autonomous taxis for hygiene concerns.

CD: What key data privacy and third-party liability concerns do these technologies raise?

Rice: These technologies utilise enormous amounts of data, which raise similarly enormous concerns about data privacy and third-party liability. Perhaps one aspect that does not get enough attention is the potential implication of litigation arising from a cyber security incident. With everyone working online, we have been seeing a huge uptick in the number of cyber attacks. Additionally, as evidenced by the Capital One lawsuit last year, there could be multimillion-dollar implications for lawsuits arising from data breaches. The software driving HAVs will have more than 100 million lines of code, making it even more susceptible to security problems. An attack on an HAV could be active, targeting the vehicles' hardware or software that manages visual information, or it could be passive, illegally gathering sensitive information for future malicious use. Moreover, because autonomous vehicles often utilise collective interlinking, a hacker would potentially be able to access a collected network and compromise multiple vehicles at the same time.

CD: Given that highly automated and connected vehicles will amass vast amounts of data, often via cloud-based services, what data security considerations do manufacturers need to make?

Rice: The good news for manufacturers of HAVs is that they are not alone in battling data security incidents. Many of the same security practices that other companies with complex infrastructures implement are equally applicable to manufacturers of HAVs. For example, all companies should conduct frequent internal security testing, such as simulating cyber attacks on their own products. Often, other companies, including vehicle manufacturing companies like GM, will employ security experts to break into their infrastructure and expose vulnerabilities. For companies that rely on cloud-based software, there needs to be a data-mapping exercise to identify sensitive data types and where it resides, and implement policies on which data types can go into the cloud and which cannot. Some adopters of the cloud have been too quick to move all their data there, only to realise it needed to be kept on-premises in a private cloud.

CD: What particular risks does the emergence of Internet of Things (IoT) technology represent, as far as highly automated and connected vehicles are concerned?

Rice: IoT ransomware is a particular risk for HAVs. IoT devices are fantastic but they pose a great deal of cyber security risks. One cyber security firm in the UK was able do a basic security scan of a wind farm and shut down every turbine. A security breach in any one HAV vehicle could be extremely disruptive – if hackers found a way to infiltrate the system, they could disrupt an entire ecosystem of ride-hailing or package delivery vehicles. In fact, the FBI has already issued a warning to the auto industry regarding this risk. For many IoT devices, the weak links are in industrial control systems, where each device is not properly defended and secured. Luckily it appears that manufacturers of HAVs are designing their vehicles with security in mind, and if they are not, they need to be.

"A security breach in any one HAV vehicle could be extremely disruptive – if hackers found a way to infiltrate the system, they could disrupt an entire ecosystem of ride-hailing or package delivery vehicles."

Tatiana Rice,
Shook, Hardy & Bacon L.L.P.

CD: What additional challenges do you expect to see highly automated and connected vehicles bring for

users and regulators in terms of road safety, security, traffic law, access to data, protection of personal data and financing?

Rice: We predict additional challenges surrounding regulations and enforcement actions aiming to prevent AI-based misidentification and discrimination by the vehicles. In the US, for example, more states are attempting to pass regulations that would require performance audits on facial recognition software to check algorithmic biases against certain subpopulations and demographics. The Federal Trade Commission (FTC) has also attempted to bring enforcement actions against companies using AI for algorithmic biases that result in unfair trade practices. This is a difficult situation to regulate, however, because the user of the software is often not the developer of it, though it is the developer who has created a model that does not adequately represent the world. There are various methods for companies to detect and assess algorithmic bias, and some companies, such as RoboFlow.ai, make it easier for developers to check the 'health' of their model to avoid over or under representations – all of which can be used to demonstrate diligence to regulators. With one self-driving car dataset, RoboFlow.ai was able to identify incomplete data sets for 33 percent of the data used to create AV algorithmic models. Nonetheless, regulators and government agencies will still face challenges on how AI-based misidentification and discrimination will be enforced and whether users of discriminatory software should be liable.

CD: What advice would you give to manufacturers in terms of establishing an appropriate data privacy law compliance solution – one that is up-to-date with regulatory and legislative developments?

Rice: We would highly recommend having at least one person in-house, or retain outside counsel, to track these developments and how they could be impacting corporate practices and policies. These regulations are often complex and demand dedicated personnel to understand the nuances and implications.

CD: As automation continues to evolve, do you expect data privacy and third-party liability complexities to increase exponentially? What steps do manufacturers need to take now to prepare for the future?

Rice: Data privacy and third-party complexities will continue to increase. The law has not yet caught up to advances in technology, but there is pressure to do so. The recent US congressional hearings, however, evidence that lawmakers not only do not understand tech, but also view tech

as the new threat to society. As a result, there will be more pressure for increased protection and liabilities as means to keep technology companies in check. In fact, we are already seeing a good deal of states pursuing greater data privacy protections in light of contact tracing concerns. The best thing manufacturers of autonomous vehicles can do right now is to test as much as possible and over-document every precaution taken – this will help defend against any allegations by regulators or plaintiffs that the company did not meet some standard of care in manufacturing and deploying their product. CD