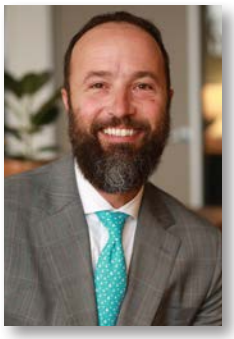
Hide and Seek in the World of Autonomous Vehicle Discovery

By Brett Schreiber

What follows is a story of cover-up and intrigue: how dogged discovery, a series of motions to compel, a pinch of luck, and the assistance of an unconventional consultant can ultimately confirm a truth we all know in the digital world – *nothing* is ever deleted. No matter what a defendant tells you, how they attempt to placate you, humor you, and at times even make fun of you, know that this truth is self-evident and when proven has the opportunity to result in significant evidentiary, and/or financial sanctions against car companies that hide the ball of digital data.



Brett Schreiber leads Singleton Schreiber, LLP's Personal Injury and Wrongful Death practice group, representing individuals and families who have been harmed by the wrongful conduct of others. He has successfully litigated and tried to verdict numerous complex cases involving automobile accidents, defective products, medical malpractice, and dangerous roadways. His trophy cabinet is filled plenty of super duper lawyer awards but his proudest title is "best dad ever," according to his four kids. Guided by the Hebrew principle of *tikkun olam*, meaning "to heal the world," Mr. Schreiber volunteers his time with numerous civil justice and philanthropic causes recognizing that a lawyer's greatest impact is often made not in the courtroom, but through the tireless work done outside of it to strengthen communities, expand access to justice, and improve lives. www.singletonschreiber.com

Please note that this is a work of fiction. All names, characters, places, and incidents are either the product of the author's imagination or used in a fictitious manner. Any resemblance to actual persons, living or dead, or actual events is purely coincidental. Nothing here should be construed to run afoul of any potentially draconian protective orders. Thus, any references to a cheesehead-wearing, chainsaw-wielding megalomaniac are not intended nor should they be suggested to reference an actual person who may or may not be leading a large but rapidly declining electric vehicle manufacturing company.

The story

It was a tragic and unfortunate crash that happened on a rural two-lane road in a tropical locale. A young couple was sitting outside their vehicle, lawfully parked, when suddenly an out-of-control Level 2 autonomous vehicle flew through an intersection, disregarding a stop sign, a limit line, and a flashing light at the end of the roadway, and collided with them without ever touching the brakes. She was killed, her boyfriend seriously injured.

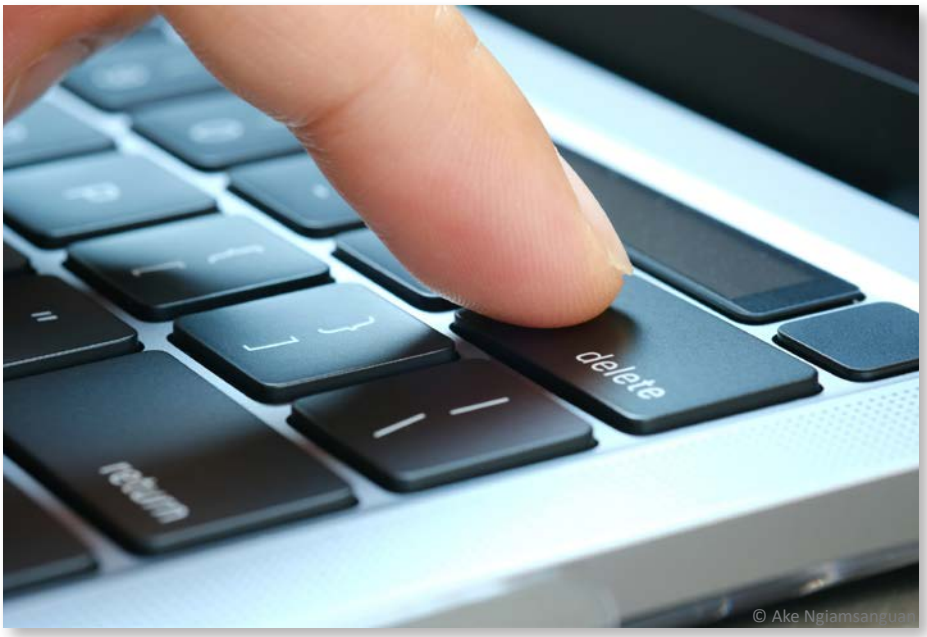
Long before civil litigation commenced against the vehicle manufacturer, a criminal investigation of the driver began. During that time, law enforcement investigated the case as a serious felony. Vehicular manslaughter causing death. Law enforcement adeptly asked the manufacturer for the hardware and software components that would likely hold relevant data and information from the advanced driver assistance system (ADAS) computer.

However, this manufacturer (like many) touts the fact that it is able to send and receive data from its vehicles over the air. Accordingly, when law enforcement sought production of information from the manufacturer, what they were sent was a series of files received at the manufacturer's mothership over the air after the crash.

To put this in perspective, the basic files received after a crash over the air are similar to the very rough outline of the book. Think of it more like the table of contents – sure it tells you the general structure of the storyline, but you don't understand the true arc and context of the narrative unless you read the chapters.

Manufacturers know there are limitations to transferring data over the air. The first is whether or not a crashed vehicle will even have a cellular connection. Recognizing that there will be circumstances where this doesn't happen, the vehicles are engineered with a workaround. Rather than first uploading the information over the air, the various data streams of what, when, where, and how the crash occurred are downloaded to the ADAS computer chip. If you think about it, this makes sense. In the moments after the crash and before the dust settles, the vehicle has no idea whether or not it will continue to have a cellular signal.

The vehicles are designed to essentially create a zip file download – a package of various data streams, including whether various system states were activated, how the vehicle was being operated, and what happened in the moments before impact. This information gets downloaded to the ADAS computer and then, much like your



The zip file may be deleted from the computer, but the truth is that nothing is ever deleted.

email refreshing itself, the vehicle checks to see if in fact it has a cellular connection, and if it does, will then transmit that zip file over the air back to the mothership.

Once the zip file is transmitted, the information is deleted from the ADAS computer. Additionally, like your fax machine from the 1990s, when the zip file is successfully transmitted to the server of the mother ship, a line of code is embedded into the computer acknowledging "transmission successful." And while the zip file may be deleted from the computer, the truth is that nothing is ever deleted. Rather, it is marked as free space on the computer's hard drive. Just like when you delete a photo from your phone, it's not actually deleted, but rather the space on your phone's hard drive is marked as free. When you then proceed to take additional photos, they overwrite that same location, essentially filling up what was free space. This is basic data infrastructure; true across platforms and devices. However, in the context of a vehicle ADAS computer, the question becomes, "how do you retrieve this information from the computer after a crash?"

The cover up

Everyone handling auto product defect litigation knows that vehicles and their component parts can disappear with the passage of time. In this story, the vehicle was ultimately found, eventually purchased by one of the litigants, but the ADAS computer was missing. After years of litigation requests and inspection, the vehicle manufacturer claimed that it had received little to no information over the air after the crash. In fact, its corporate designee witness testified in numerous cases across the country that it is very common for the company to only receive partial over-the-air uploads after a crash. One stream of data here, another stream of data there.

In fact, the company had received the data on how and why the crash occurred before the plaintiffs had been transported from the scene via ambulance.

Despite subpoenaing multiple law enforcement agencies, deposing numerous company witnesses and making repeated demands of the manufacturer no one was able to locate the vehicle's ADAS computer. Eventually, a deposition of a little-noticed evidence custodian was taken when inquiry was made as to the location of the components. It was confirmed that the computer was being stored in a facility that no one had ever thought to check. Previous subpoenas had turned up nothing, and yet the storage clerk pointed lawyers in the right direction. A day later, an evidence log ticket was pulled and the computer components were found on a dusty shelf in the corner. Eureka, they had found it! The problem was the manufacturer assured the parties and the court that it was impossible to decipher information directly from the ADAS computer itself. It had to be connected to a vehicle, it had to receive software updates and only the manufacturer had the tools to get it done. Or so they said.

Several months of back-and-forth ensued with the manufacturer demanding that the computer be plugged into a new vehicle, the software updated, and any data received sent over the air to the manufacturer's servers. Fortuitously, at that same time, an intrepid reporter from a national publication had taken a deep dive into this manufacturer's efforts to hide and withhold data from the federal government. This reporter was able to locate a hacker who had spent years taking apart exemplar motherboards to understand how the vehicle's ADAS computer worked. He ultimately had developed a technique from crashed vehicles where he would pull the computer, remove the chip from the computer, extract the data and oftentimes post his findings on Twitter.

After numerous direct messages on Twitter and with the help of the reporter, the hacker eventually agreed to consult with the attorneys involved. He was reluctant to engage in litigation; after all, he was afraid that it would impact his ability to continue his probing of the car company's systems. But he nevertheless agreed.

continued on page 22

Autonomous Vehicle Discovery

continued from page 17

Motions to compel followed and the manufacturer was ultimately ordered to produce the data from the ADAS computer. The plaintiffs, with their hacker in tow, pulled the data themselves directly from the chip off the computer. The irony was lost on no one when the plaintiffs and their hacker were the ones deciphering the manufacturer's own data from its own computer. Once received, the manufacturer claimed all the data was a series of empty folders. They didn't even understand what they had. Only with the help of the hacker did the manufacturer come to realize that all of the files could be undeleted.

And suddenly, for the first time in four years of litigation did the ground truth – i.e. how the crash occurred in both time and space – finally become clear. Additionally, so too was the line of code showing that the manufacturer had successfully received this data over the air within moments of the crash four years earlier. In fact, the company had received the data on how and why the crash occurred before the plaintiffs had been transported from the scene via ambulance. Nevertheless, through efforts coordinated by in-house counsel, the company continued to claim it never received the data.

Since the data clearly showed the how and why of the system failure, it's no wonder the manufacturer denied receiving it. A motion for sanctions followed. The court ultimately awarding hundreds of thousands of dollars in monetary sanctions against the defendant. It can certainly be argued that the manufacturer, a company whose value is higher than 99.9% of companies in the world, will not be dissuaded by a modest six-figure monetary sanction.

However, for the first time, this manufacturer and others like it now know that outsiders can analyze, interrogate, and understand their data infrastructure. Sometimes better than the manufacturers themselves. Will this cause them to behave better? Probably not. But if they do continue to hide their digital data, there is a path forward for holding them accountable. It can be proven. It can be traced. Because remember, *nothing* is ever deleted. ■