

TESLA MOTORS LIES TO THE PUBLIC AND THE COURTS

Tesla said it didn't have key data in a fatal crash.
Then a hacker found it.

The critical evidence was presented last month to a jury, which found the company partially liable for the 2019 crash in Key Largo, Florida.

By Trisha Thadani
and
Faiz Siddiqui

Years after a Tesla driver using Autopilot plowed into a young Florida couple in 2019, crucial electronic data detailing how the fatal wreck unfolded was missing. The information was key for a wrongful death case the survivor and the victim's family were building against Tesla, but the company said it didn't have the data.

Then a self-described hacker, enlisted by the plaintiffs to decode the contents of a chip they recovered from the vehicle, found it while sipping a Venti-size hot chocolate at a South Florida Starbucks. Tesla later said in court that it had the data on its own servers all along.

The hacker's discovery would become a key piece of evidence presented during a trial that began last month in Miami federal court, which dissected the final moments before the collision and ended in a historic \$243 million verdict against the company.

The pivotal and previously unreported role of a hacker in accessing that information points to how valuable Tesla's data is when its futuristic

technology is involved in a crash. While Tesla said it has produced similar data in other litigation, the Florida lawsuit reflects how a jury's perception of Tesla's cooperation in recovering such data can play into a judgment in the hundreds of millions of dollars.

The company's driver-assistance technology includes features that automatically control a Tesla's speed and steering, and are programmed to react when an obstacle, such as another vehicle or a pedestrian, is in its path. Tesla CEO Elon Musk has referred to its vehicle as a "very sophisticated computer on wheels" and said Tesla is a "software company as much as it is a hardware company." He has positioned the company's most advanced iteration of driver-assistance available to consumers, Full Self-Driving, as "the difference between Tesla being worth a lot of money and being worth basically zero."

The batch of data the plaintiffs were after, internally referred to as a collision snapshot, showed exactly what the vehicle's cameras detected before the crash, including the young woman who was killed. The plaintiffs' attorneys said they believed the data would present a damning picture of the system's shortcomings, and the hacker — who for years had been taking Autopilot computers apart and cloning their data — was confident he could find it.

"For any reasonable person, it was obvious the data was there," the hacker told The Washington Post, speaking on the condition of anonymity for fear of retribution. The hacker, known online by his X handle @greentheonly, did not testify in the case.

e

ped

Plaintiffs construct a more detailed version ahead of trial. (Video: Obtained by The Washington Post)

r

o

r

Over three weeks in Miami, a jury was asked to consider how much Tesla's Autopilot technology was to blame for a crash that killed 22-year-old Naibel Benavides Leon and catastrophically injured her boyfriend, Dillon Angulo, in Key Largo. The plaintiffs filed a joint federal lawsuit against Tesla last year, alleging that the vehicle failed to alert the driver to the couple ahead and was negligent in allowing Autopilot to operate on a road for which it was not designed.

Angulo and the Benavides Leon family initially sued the driver of the Tesla, George McGee, who said he was using Autopilot when he looked away from the road to retrieve a dropped cellphone. McGee, who settled with the plaintiffs in a separate case, did not respond to a request for comment. Tesla said that it was not responsible for the crash and that McGee was fully to blame, because the law and its owner's manual state the driver must be in control, no matter whether Autopilot is engaged. The company also said it did not intentionally suppress the key data, but rather simply couldn't find it.



Follow Technology

Joel Smith, Tesla's attorney, said in an interview that the company was "clumsy" in its handling of the data but did not engage in any impropriety with regard to it. "It is the most ridiculous perfect storm you've ever heard," Smith said, in an effort to explain why Tesla was unable to produce the collision snapshot data until after the hacker retrieved it for the plaintiffs.

In court, Smith told jurors in his opening statement that Tesla would "never think about hiding" the data because it proved that the driver had

time to react to the pedestrians standing by their parked car had he been paying attention.

“We didn’t think we had it, and we found out we did,” he said. “And, thankfully, we did because this is an amazingly helpful piece of information.”



It took the jury less than a day of deliberation to find Tesla 33 percent liable for the crash and responsible for \$243 million in punitive and compensatory damages. The verdict was a stunning setback for a company that for years has successfully argued that the driver bears the responsibility when its technology is involved in a crash. Tesla said that the verdict was wrong and that it plans to appeal, given the “substantial errors of law and irregularities at trial.”

U.S. District Judge Beth Bloom, who presided over the case, said in an order that she did not find “sufficient evidence” that Tesla’s failure to initially produce the data was intentional. She ruled, however, that Tesla was required to reimburse the plaintiffs for all the costs related to retrieving the data themselves. A person with knowledge of the case and

the company's thinking, speaking on the condition of anonymity to discuss sensitive matters, said that despite the judge's finding, the dispute over the data's accessibility is likely to have had a "significant impact on the verdict."

"This is kind of a trailblazing case," said Fred Lambert, editor in chief of the electric vehicle enthusiast site Electrek, which earlier reported the dispute around the data. Lambert said he believed Tesla's handling of the data played a part in the outcome, adding that the case could have played out differently "if they were able to drag this on a little longer, or the plaintiff couldn't have managed to get the Autopilot [computer] cloned in time."

Already, the impact of Tesla's loss is reverberating beyond the Miami courtroom.

A shareholder lawsuit in Texas filed this month alleges Tesla defrauded investors with its promotion of autonomous driving technology. The shareholder complaint specifically cites the outcome of the Florida case before accusing Tesla of "wrongful acts and omissions." Experts said the verdict has also given fresh momentum to pending cases across the country, including one expected to go to trial in Northern California in the fall over the death of a 15-year-old.



In interviews, Angulo and Benavides Leon’s sister, Neima Benavides, said they passed up “a lot of money” from Tesla, which they said tried to avoid trial by offering them a confidential settlement. Tesla declined to comment, though settlement offers are not unusual in such cases. Aware they faced a tough defense, the plaintiffs said they wanted the public to know how Tesla deceived them in the years following the crash — including the prolonged battle over the data eventually recovered by the hacker.

“We have this relief that the world knows, but it doesn’t change anything for us,” Neima Benavides said. “My sister is not here. And nothing will bring her back.”



‘Corrupted’ data

Immediately after the wreck at 9:14 p.m. on April 25, 2019, the crucial data detailing how it unfolded was automatically uploaded to the company’s servers and stored in a vast central database, according to court documents. Tesla’s headquarters soon sent an automated message back to the car confirming that it had received the collision snapshot.

Moments later, court records show, the data was just as automatically “unlinked” from the 2019 Tesla Model S at the scene, meaning the local copy was marked for deletion, a standard practice for Teslas in such incidents, according to court testimony.

In the time between the crash and the hacker’s intervention, according to testimony from a software engineer and manager on the Autopilot team, someone at Tesla probably took “affirmative action to delete” the copy of the data on the company’s central database, too, leaving investigators and the family without the information they believed they needed to piece together what happened.

About two months after the crash, Cpl. David Riso, then the Florida Highway Patrol’s lead traffic homicide investigator, walked into a Tesla service center in South Florida — a meeting arranged by one of Tesla’s lawyers — holding two parts from the mangled Tesla, court records say: the media control unit, a flat center screen used for navigation and other features, and the Autopilot control unit, a metal box that housed the crucial data and had cables hanging off it.

From there, a Tesla service technician worked to retrieve the information he could — plugging the media control unit into a different Tesla and surveying its contents on a computer.

That employee attested that he never powered on the Autopilot control unit, where the snapshot resided, court documents show, and focused on the media control unit instead. But according to documents, Tesla acknowledged that the Autopilot control unit transmitted data at the time of the police inspection. Tesla recanted its employee's testimony "after discovering evidence inconsistent with his stated recollection of events," it said.

Powering up that unit posed a major problem, said Alan Moore, an expert witness and forensic engineer who testified for the plaintiffs, launching "a number of automatic processes," which can include updating software. "The problem is ... all of this is happening in the treasure trove," he said, putting the collision snapshot at risk.

At the service center that day, the service technician downloaded data to a thumb drive Riso had brought to the facility. But the employee immediately set expectations low, Riso told the jury last month. He "told me it was corrupted even before he handed the thumb drive [back] to me," Riso said in his testimony.

After years of trying and failing to retrieve this data from Tesla, the plaintiffs' attorneys said, they finally hit a wall in 2024 and were preparing to go to trial without it. But in a last-ditch effort to find the snapshot that summer, they recovered the control units from the Florida Highway Patrol, which still had them in its possession. Then they needed a technical expert to understand and extract what was on them.

That's when they turned to hacker greentheonly, who had a robust social media following for his work recovering data from damaged Teslas and posting his findings on X.

The hacker was consulting with the plaintiffs' team when Tesla proposed to the plaintiffs that they power on the Autopilot control unit to determine what data it held — an idea greenetheonly vehemently opposed.

“Let's just power it on and update [it] and see what happens,” he recalled them suggesting. “If I wanted to destroy evidence on the computer, that would be exactly the advice I would give.”

After a lengthy back-and-forth, Tesla and the plaintiffs agreed on terms for the hacker to access the data from the Autopilot unit himself. In October, the plaintiffs' attorneys flew the hacker down to Miami from his home hundreds of miles away.

Inside a Starbucks near the Miami airport, the plaintiffs' attorneys watched as greenetheonly fired up his ThinkPad computer and plugged in a flash drive containing a forensic copy of the Autopilot unit's contents. Within minutes, he found key data that was marked for deletion — along with confirmation that Tesla had received the collision snapshot within moments of the crash — proving the critical information should have actually been accessible all along.

The attorneys high-fived behind him.





Over the next few days, the hacker used the data he had found to create an augmented video of the crash that showed in stark detail exactly what the Tesla saw in the moments before the crash.

In the annotated video played for the jury, the vehicle detects a vehicle about 170 feet away. A subsequent frame shows it detecting a pedestrian about 116 feet away.

As McGee hurtles closer and closer, the video shows the Tesla planning a path through Angulo's truck, right where he and his girlfriend were standing behind signs and reflectors highlighting the end of the road.

In court, Smith, Tesla's attorney, said the video was a clear illustration of how McGee had plenty of time to react had he been paying attention to the road. Smith said Tesla would have loved to have this evidence all along but had not been able to locate it.

Brett Schreiber, the plaintiffs' lead attorney, had a different interpretation, saying that the vehicle failed to warn McGee the road was ending — and that Tesla had deceived the investigators for years about what data was available even though the company had it “before the cops even arrived on the scene.”

“There’s too much going on here for it to be anything other than intentional,” another plaintiffs’ attorney, Adam Boumel, said in an interview.





‘The facts are a stubborn thing’

Federal regulators have ordered investigations and recalls of Tesla’s vehicles after dozens of serious crashes, including fatalities, over the past decade. Experts and lawyers with similar Autopilot-related cases said verdicts like the one in Miami are perhaps the only way to hold the company accountable in the public eye as Musk continues to deploy its evolving and experimental technology on the roads.

The Miami verdict “gives us future hope that these can be successful,” said Don Slavik, a products liability attorney who has several pending cases against Tesla. “The message from the jury is that ‘You did something wrong, change what you’re doing.’ But until we see that occur, I’m afraid that it is going to take additional verdicts.”

Tesla has twice beat lawsuits alleging design flaws in court and settled at least four other cases before they made it to trial. The troves of newly

revealed evidence in the Miami case, including the transcriptions from hours of testimony, provide an unprecedented look into Tesla's playbook for defending itself in court.

The case also continued a string of recent defeats for Tesla on claims related to its advanced driver-assistance systems.

In a landmark ruling in June, Marc Dobin, an attorney based in Washington state, won an arbitration award entitling him to a full refund for his \$10,600 purchase of Tesla's Full Self-Driving technology after an arbitrator ruled that Tesla had failed to deliver the promised features. In mid-2021, Dobin bought a 2021 Tesla Model Y with a software package but was never able to access what Tesla then called Full Self-Driving Beta before trading in the vehicle in March 2022.

That and the 2019 crash, as Dobin sees it, are examples of Tesla overpromising. "The problem with the Key Largo case — and this is where it all ties together — is Elon Musk's big mouth," he said.

The company declined to comment for this article beyond authorizing its lawyer to discuss the case.

Meanwhile, several pending lawsuits against Tesla related to fatal and serious crashes are expected to go to trial in the next few years. Schreiber — the plaintiffs' attorney in the Miami case — is expecting to face the same defense team this fall in California for another Autopilot-related case involving the death of a 15-year-old boy. With fresh confidence gathered from his recent verdict, Schreiber said he has "every intention" of asking the next jury he faces for a verdict "north of a billion dollars."

"The facts are a stubborn thing," Schreiber said.



Greentheonly, the hacker who helped recover the data in the Miami case, continues to probe Tesla Autopilot computers from a basement workshop strewn with circuit boards and soldering equipment.

That work is only becoming harder, he said, as Tesla is tightening the controls over access to vehicle crash data. “If an accident happened today like this, I won’t be able to extract the data,” he said.

He is convinced that Tesla’s reactive posture to data surrounding crashes is a flaw. “Sometimes,” he said, “you just have to get the data out.”