Autonomous Vehicles Are Driving Blind

In San Francisco this month, a woman suffered traumatic injuries from being struck by a driver and thrown into the path of one of hundreds of self-driving cars roaming the city's streets. San Francisco's fire chief, Jeanine Nicholson, recently testified that as of August, autonomous vehicles interfered with firefighting duties 55 times this year. Tesla's autopilot software, a driver-assistance system, has been involved in 736 crashes and 17 fatalities nationwide since 2019. (…)

The reason is simple: There are no federal software safety testing standards for autonomous vehicles — a loophole large enough for Elon Musk, General Motors and Waymo to drive thousands of cars through. The National Highway Traffic Safety Administration regulates the hardware (such as windshield wipers, airbags and mirrors) of cars sold in the United States. And the states are in charge of licensing human drivers. To earn the right to drive a car, most of us at some point have to pass a vision test, a written test and a driving test.

The A.I. undergoes no such government scrutiny before commanding the wheel. In California, companies can get a permit to operate driverless cars by declaring that their vehicles have been tested and the "manufacturer has reasonably determined that is safe to operate the vehicle." (…)

A.I. often makes surprising mistakes. (…) Last year, an autonomous car slammed on its brakes while making a left turn because it seemed to have thought that an oncoming car was going to make a right turn into its path. Instead, the oncoming vehicle slammed into the stopped driverless vehicle. Passengers in both cars were injured. (…)

Of course, the problem isn't limited to cars. Every day we learn a different way that the A.I. chatbots are failing — whether by inventing case law or by sexually harassing their users. And we have long been grappling with the failures of A.I. recommendation systems, which at times have recommended gun parts and drug paraphernalia on Amazon, which restricts such items, or pushed ideologically biased content on YouTube.

Despite all these real-world examples of harm, many regulators remain distracted by the distant and, to some, far-fetched disaster scenarios spun by the A.I. doomers — high-powered tech researchers and execs who argue that the big worry is the risk someday of human extinction. (…)

In the United States, a wide array of A.I. legislation has been proposed in Congress, largely focused on doomer concerns, such as barring A.I. from making nuclear launch decisions and requiring some high-risk A.I. models to be licensed and registered.

The doomer theories are "a distraction tactic to make people chase an infinite amount of risks," says Heidy Khlaaf, a software safety engineer who is an engineering director at Trail of Bits, a technical security firm. (…)

In other words, we need to start acknowledging that A.I. safety is a solvable problem — and that we can, and should, solve it now with the tools we have.

Experts in different domains need to evaluate the A.I. used in their fields to determine whether it is too risky — starting with making a bunch of autonomous cars take vision and driving tests.

It sounds boring, but that's exactly what safety is. It is a bunch of experts running tests and making checklists. And we need to start doing it now.

Julia Angwin, *The New York Times,* October 11, 2023.