TechScape: Self-driving cars are here and they're watching you

Publication Date: 2023-07-04

Author: Johana Bhuiyan

Section: Technology

Tags: Technology, TechScape newsletter, Automotive industry, Motoring, Self-driving cars, Waymo, Google, Alphabet, features

Article URL: https://www.theguardian.com/technology/2023/jul/04/smile-youre-on-camera-self-driving-cars-are-here-and-theyre-watching-you

If you've spent any time in San Francisco, you might believe we're on the cusp of the self-driving future promised by car makers and the tech industry: a high-tech utopia where roving robot cars pick up and drop off passengers seamlessly and more safely than if they had a human behind the wheel. While the city certainly has one key element down – a small network of driverless cars – the reality is far different and much more awkward and invasive than what the people building the technology once portrayed. What companies pitched were ultra-smart, AI-driven vehicles that make people inside and outside of the cars safer. But in addition to reports that the cars are becoming a frequent impediment to public safety, the always on-and-recording cameras also pose a risk to personal safety, experts say. A new report from Bloomberg reveals that one of the companies behind the self-driving cars that are operating in San Francisco, Google-owned Waymo, has been subject to law enforcement requests for footage that it captured while driving around. This is not the self-driving future we were promised – but it is the one that surveillance and privacy experts have warned about. "I see this as a perfect natural extension of automotive surveillance where for years we've had growing numbers of features that are turning our cars into policing tools," said Albert Fox Cahn, an anti-surveillance activist and director of the Surveillance Technology Oversight Project. "Now that we can no longer deny that this is going to be a way people are tracked, we have to ask if the car companies are willing to make the sort of investment it takes to prevent their cars from driving us straight into authoritarianism." Perhaps it should be no surprise that this issue would face users of autonomous vehicles. We are already witnessing the threat of surveillance technology in ways big and small, such as China's mass surveillance of Uyghurs and other ethnic minorities, and the row in 2019 over the use of facial recognition at King's Cross, in London. As the companies expand their driverless footprint outside of California to cities in Texas and Arizona, and self-driving technology begins to proliferate globally, the ways in which the companies collect, store and handle user data is critical to track. When it comes to law enforcement and user data, if a tech company collects it the warrants and subpoenas will come. And it's not just an issue facing the US. In 2022, the EU finalised a legal framework on autonomous vehicles and is expected to add a provision that manufacturers can collect data and release it to authorities. How that will play out is yet to be seen. Uneasy rider Self-driving experts and proponents have pitched the technology as a life-saving mechanism that can make streets and people safer. Waymo likes to say it is building "the world's most experienced" driver and Cruise, owned by General Motors, says it frequently conducts safety checks to ensure it can "keep riders and the communities we operate in safe". But what about personal safety? Privacy experts

warn that surveillance technology and systems which collect user data that are vulnerable to law enforcement requests disproportionately harm marginalised groups and are a violation of constitutional rights to privacy. When it comes to self-driving systems, cameras play a crucial role. The cameras on the outside of the cars help vehicles navigate the streets they're driving on and manufacturers say the cameras inside the vehicles allow them to support customers as needed. Surveillance is hard to ignore when you're in one of these vehicles. On a recent test drive of a Cruise driverless car in San Francisco, friends and I were confronted by cameras staring down at us from all directions as soon as we got into the car. One of my friends was so uncomfortable that she covered her face throughout the ride. Unsurprisingly, police have started to wise up to the potential for the footage these cameras capture to help them in investigations. In San Francisco and Arizona, Waymo had been issued at least nine search warrants for footage from their vehicles, according to Bloomberg, and Cruise had received at least one. Given these types of legal requests often come with gag orders – or mandates to not disclose the existence of the warrant – it's not clear if that is the extent of it. There's also precedent for police to ask for footage from systems that record inside and outside enclosed spaces, according to Cahn. "We already see examples of people getting police warrants for Ring camera data from both outside and within their homes," he said. "Where there's a camera, it's just, one court order away from being used against you in a court of law." Waymo and Cruise say they carefully review law enforcement requests – which they said they haven't received very many of – and only comply when necessary. For both services, users have to consent to a privacy policy before riding in one of the vehicles and both companies say they may share the footage with government agencies if asked for it. Cruise says it only saves internal footage for a "short periods of time", but doesn't go into specifics. "Privacy is extremely important to us which is why we disclose relevant data only in response to legal processes or exigent circumstances, where we can help a person who is in imminent danger," said Cruise spokesperson Navideh Forghani. How data could be weaponised Google is no stranger to law enforcement requests. The tech giant receives more than 50,000 government requests for user data every six months, but a roving surveillance camera that captures passersby who may not consent to having their activity captured is a relatively new frontier, even for Google. Many other data points could potentially land in the hands of law enforcement, including where a user gets picked up or dropped off. And Cahn notes that companies developing driverless cars may not be incentivised to push back against local enforcement authorities. But his hope is that the short-term risk of losing customers because they're afraid they will be recorded inside or near the cars is motivation enough. While the presence of cameras in a self-driving system seems unavoidable at the moment, there are mechanisms the company can implement to safeguard the footage and other user data from being weaponised against the people in and around the cars. The simplest solution is not to collect or store the data in the first place. The second option, which is not a sure-fire protection, is to collect but anonymise and de-identify the data. Finally, encrypting the footage so that only the user holds the key to access the data is a mechanism more tech companies are implementing to provide privacy protections for its users. (Neither company responded to questions about whether it would consider encrypting the data or footage.) "I'm concerned that the car makers haven't really considered privacy at all when thinking about the ways their vehicles are gonna be used to put their customers in jail and to monitor everyone they go by," Cahn said. The limits of Twitter Twitter is becoming increasingly unusable with the changes Elon Musk has implemented in the last few weeks. Most recently, after some Twitter users reported trouble viewing tweets, among other issues, Musk announced he was limiting the number of tweets people could see. Verified users would be able to view 10,000 posts a day while unverified users would only be able to see 1,000. (The limits were originally set at 6,000 and 600, respectively, but bumped up almost immediately.) Musk says the rate limits were necessary to address "data scraping" by third-parties – an issue he's complained about with regards to AI companies such as OpenAI using Twitter data to train their large language models. (Remember, Musk was an OpenAI co-founder but reportedly left the organisation after the other founders rejected his attempt to take over.) Musk's announcement sent users fleeing to other platforms including Bluesky, the Twitter rival with backing from its former CEO Jack Dorsey, and Meta is launching its Instagram-linked answer to Twitter, called Threads, on Thursday. The influx of users caused performance issues on Bluesky resulting in the platform temporarily pausing sign ups. The rate limit was also being blamed for Twitter-owned dashboard TweetDeck malfunctioning on Monday. If you want to read the complete version of the newsletter please subscribe to receive TechScape in your inbox every Tuesday.