LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
TUESDAY, DECEMBER 26, 2023

GUEST COLUMN

Ensuring transparency in autonomous vehicle regulation

By Aaron H. Jacoby and Gordon Sung

Shutterstock

The autonomous vehicles (AV) industry faced significant regulatory activity in Q4 2023, probably the most significant in its history. Much of the activity may have been driven by the perception that AV technology is overwhelming current infrastructure and oversight capabilities.

A series of mishaps in San Francisco resulted in a Dec. 1 Order to Cruise LLC issued by the California Public Utilities Commission (CPUC) to show cause why sanctions should not issue for "failing to provide complete information and for making misleading public comments." The Order focuses on the Company allegedly omitting material information during its incident reporting following an incident that occurred on Oct. 2, 2023. These developments unfolded just a few months after the CPUC's landmark decision on Aug. 10, 2023, where it granted CPUC AV Deployment Permits to both Cruise and Waymo. That Permit authorized both companies to provide and collect fares for 24/7, fully driverless (i.e., no safety operator behind the wheel) "robotaxi" service throughout San Francisco, the most expansive AV operational authorization the agency had provided to date.

The CPUC alleges in its Order that Cruise may have violated Rule 1.1 of the CPUC's Rules of Practice and Procedure, which prohibit "mislead[ing] the Commission or its staff by an artifice or false statement of fact or law." It also cites Pub. Util. Code §§ 2107 - 2108, which permits the Commission to broadly fine a public utility not in compliance with a CPUC rule, order, ruling, or regulatory requirement, $500 to $100,000, with each violation a separate finable offense, and that "each day's continuance of a violation" is considered "a separate and distinct" offense. In addition, the Order cites Pub. Util. Code §§ 5411, 5415, which specifically applies to charter-party carriers, including robotaxi operators. These code provisions allow the CPUC to impose an additional fine of $1,000 to $5,000 for each offense and, again, each day's continuance of such violation can be a separate and distinct offense. Finally, the Order cites Cal. Pub. Util. Code § 5378 as another basis to impose a $7,500 fine for each violation set forth in that particular code provision. The Order alleges that Cruise "failed to provide the [CPUC] with a full account of the ... incident for 15 days," measured from Oct. 3, the day it first reported the incident and allegedly omitted material information, to Oct. 18, the day it first told the CPUC that it would provide a longer video of the incident, the existence of which the Order notes was learned about during meetings between the CPUC and the California DMV. As you can see, under the CPUC's penalty theories, the exposure from a single incident can compound quickly. This is not unique to CPUC practice and, in fact, is common across state and federal enforcement authorities.

Key considerations for interactions with regulators

Typically, transparency with regulators is the key to successful resolution of any inquiry. Consistently and effectively demonstrating transparency requires well designed internal policies and processes. Transparency enables parties to address investigations and minimize penalties (assuming no serious or criminal misconduct that would warrant severe penalty). Transparency means that sufficient information is provided to allow an investigator to feel comfortable that the regulated entity has provided all relevant information to which the regulator is entitled. Achieving this result is not a matter of good intentions

or "culture," a popular phrase frequently used by commentators. As the CPUC's Order illustrates, the moment a request has been issued by a government regulator the clock begins to tick. Without experienced personnel and effective policies in place, AV companies risk creating bad facts early in the process that can snowball.

Companies developing AV technology and other nascent technologies with safety components (e.g., artificial intelligence deployed to automate real-world decision making), have unique challenges. Most in the industry view themselves as good actors developing safe technology responsibly and fully desire to be transparent and collaborative with regulators. On almost every AV company's website there will be some version of the phrase somewhere that "safety is core to our culture." Regulators generally view themselves as fair and balanced protectors of public safety who do not unduly hinder innovation. Unlike other more established industries, however, AV regulators are still learning the technologies that they are charged with overseeing. Similarly, companies developing emerging technologies do not have many historical regulatory enforcement precedents to draw from. In short, both sides lack the wisdom and benefit of time. Contrast this situation with starting a new hedge fund, for example, which can look to countless Securities and Exchange Commission (SEC) consent orders to develop a hiring plan for their legal and compliance functions who in turn can establish market compliance policies and practices. Similarly, a new automotive manufacturer can draw from over 50 years of Vehicle Safety Act precedents when making decisions about which safety standards it will follow for each component of the vehicle they are developing. This is not the case in the AV industry.

How should AV and other emerging technologies develop the processes needed to ensure transparency with regulators? Below we provide some high-level suggestions. In short, it will require multidisciplinary expertise and collaboration with experienced legal, compliance, and safety engineering professionals.

Amongst the lowest-hanging-fruit policies that companies in this space should evaluate are its Code of Ethics and data retention policies.

Code of Ethics policies make explicit that all employees are expected to help the company stay in compliance with all laws and regulations. They are standard in highly regulated industries that regularly respond to government inquiries. They require all employees to respond to any request from the company's legal or compliance department promptly, honestly, and completely. In companies with strong legal compliance cultures, all employees, from the CEO down, may be required to regularly (i.e., at least quarterly) be trained in the policy, asked to certify their understanding, and affirm that they will comply. Violations of the policy should be potentially severe, documented, and consistently applied. Code of Ethics policies, if implemented properly, have the effect of establishing a company culture that its lawyers, professionals trained and ethically bound to duties of candor, will drive its response to a government inquiry. It is not the job of any employee to "help" the company get out of the government inquiry unscathed - their only job is to be transparent during internal inquiries and follow the experienced legal professionals' lead in external-facing responses.

For AV companies, it is particularly important for engineering leadership, operations teams, and government relations personnel (i.e., the teams responsible for the initial gathering of information following an incident) to be trained in the Code of Ethics policy. Bad facts can be created early in the process if team members on the ground feel pressure to make the "right decision" that will protect their employer, colleagues, or manager, as opposed to sticking to their obligations under the Code of Ethics and following the company's lawyers who, again, are trained and bound by ethical duties of candor.

A formal and consistently applied data retention policy is critical as well. Many AV companies likely have some form of data retention policy in place that focuses on technical requirements (e.g., to control data storage costs). It would be prudent to review such policies with the company's legal advisers to understand how they would be viewed in a government investigation and make any necessary revisions. A common and easily avoidable problem when responding to a government inquiry is if the company has deleted information that the regulator deems relevant without being able to show that the deletion was pursuant to a clear, reasonable, and responsible policy, and done in the regular course of business (i.e., not to hide information).

Finally, AV companies should work with multidisciplinary experienced professionals, including dedicated-safety engineering and legal advisors, to develop technology release policies with concepts borrowed from other safety-critical industries, such as aerospace, aviation, and traditional automotive. Common questions asked by safety regulators surround the company's testing protocols before determining if a technology is safe to be released into the real-world, and whether such policies were followed.

We note that none of the suggestions contained herein should be considered a criticism of how Cruise handled the Oct. 2, 2023, incident. Any serious safety incident will test even the best prepared company's response protocols. Well-designed safety and incident response policies, especially in an emerging technology, recognize that it is impossible to anticipate every possible real-world consequence of an incident. Rarely are decisions black-and-white, and a rush to judge how a technology behaved or a company's response in a pioneering industry may not be fair to the company's rights to due process or in the public's long-term interests.

Aaron H. Jacoby *is managing partner of the Los Angeles office of Arent-Fox Schiff, LLP, and* **Gordon Sung** *is counsel in the San Francisco office.*