

NEWS & INSIGHTS

Denuclearization Part 7: The Data Dilemma - How the Discovery Fallacy is Costing You Cases

BY: [DOUGLAS B. MARCELLO](#) | [INSIGHTS](#) | [ARTICLE](#)

MAY 14, 2026



Note: This is Part 7 of the “Denuclearization” series. You can read [Part 1 here](#), [Part 2 here](#), [Part 3 here](#), [Part 4 here](#), [Part 5 here](#), and [Part 6 here](#).

The One Big Thing

Plaintiff attorneys have a name for your safety data. They call it a treasure trove. At their seminars and webinars, they teach each other what you have, how to get it, and how to make it admissible. The goal is to leverage your own data against you; to take the information you collected to make your operations safer and use it to secure a verdict. Actually, inflate a verdict.

Too many carriers respond to this reality with what I call Discovery Fallacy, the belief that if you don't look at your data, you won't have to turn it over. That avoiding analysis is the same as avoiding exposure.

The Discovery Fallacy is wrong, and it is one of the most dangerous mistakes in trucking defense. The data exists whether you look at it or not. The question is not whether plaintiff attorneys will find it. The question is whether you got there first, whether you created the narrative, or abdicated it to them.

Because the narrative they create will not be very pretty.

Why It Matters

The Data Dilemma sits at the center of the Denuclearization framework. We covered the [Reptile Theory in Part 6](#), how plaintiff attorneys transform individual accidents into systemic community safety indictments. Your safety data is the ammunition for that strategy. Telematics records, electronic control module data, collision avoidance system alerts, communication logs, driver performance scores: All of it is discoverable, all of it is potentially admissible, and all of it can be weaponized if you haven't managed it proactively.

But here is what too many carriers miss: The same data that plaintiff attorneys want to use against you is the data that can defend you, if you have identified it, analyzed it, managed it, and enforced against it before the accident happened. A carrier that can walk into court and show a documented pattern of identifying risk indicators, addressing them systematically, and holding drivers accountable has a fundamentally different defense than one that learned what its data said for the first time in discovery.

The choice is yours. You can create your narrative, or you can abdicate it to the plaintiff attorneys. The data does not care either way.

The Framework: Four Steps That Change the Defense

Managing your safety data for litigation defense is not complicated. It requires four things, in order:

- **Identify.** Know what data you have. This sounds obvious, but many carriers don't fully know what data they are generating until after an accident, when they're working with an accident reconstructionist to find out. Telematics. Electronic control modules. Collision avoidance systems. Communication records. Driver performance platforms. Know your data landscape before you need it.

- **Analyze.** Once you know what you have, understand what it means. Different operations generate different risk signals. A carrier running I-80 in Nebraska is going to see different primary indicators than one running the George Washington Bridge into New York. Know what the key indicators of crash potential are for your specific operations and routes, because those are exactly what plaintiff counsel will focus on.
- **Manage.** Monitor the key indicators you've identified and take documented action to reduce the conditions that create accident potential. This is where analysis becomes defense. A carrier that can show it was monitoring its own risk data and responding to it is a carrier that defeats the systemic failure narrative.
- **Enforce.** This is the hardest step. In a tight driver market, enforcement means difficult conversations and sometimes losing drivers. But ask yourself: how many safe miles do your good drivers have to run to pay for one bad actor's verdict? Or worse: will that one bad actor be an existential threat to your business? Documented enforcement is the final piece of the defense. It shows the jury that when the data identified a problem, the company acted on it.

What to Watch

[The DataQs reform we previously covered](#) is directly connected to this framework. Your FMCSA inspection and crash data is the external safety record that plaintiff attorneys access first, via the [Freedom of Information Act \(FOIA\)](#), before the lawsuit is even filed. The DataQs reform gives you a better mechanism to challenge inaccurate records in that external database. You must also consider the internal safety data that your own systems generate. Both records matter. Both need to be managed.

If you or your company have questions about how to proactively prevent Discovery Fallacy, please [contact me](#) or any member of the [Saxton & Stump Trucking and Commercial Transportation Group](#).

Coming up: Part 8 of the Denuclearization series addresses Anchoring and Non-Economic Damages: How the damages structure in nuclear verdict cases gets built, and what defense counsel can do to counter it.

Related People

[Douglas B. Marcello](#)

Related Services and Industries

[Trucking and Commercial Transportation](#)