NOTES·THEPOSITION

Whose data is it?

Across auto retail, restaurant tech, and delivery, vendors have fought to keep operators from the data their businesses produce. The pattern, documented, and the position we build from.

YYZDATA·AUGUST2026

An operator asks the company that runs their point of sale for access to their own data. What comes back is a rate card, a tier upgrade, or silence. Anyone who has run a venue recognizes the conversation. It reads like an edge case until you line the industries up, and then it reads like a business model.

Auto retail is the documented extreme. Sworn testimony recorded a DMS vendor raising its data-integration charge from $247 to $893 per dealer per month for reaching data the dealership generated, and the resulting antitrust litigation settled for $630 million, $100 million, and $29.5 million across the two dominant vendors. (Authenticom v. CDK Global, 7th Cir. record; settlement filings 2024-2025) The full account is in our note, The $893 line item.

Restaurant technology runs a softer version of the same trade. Access to advanced reporting on your own sales is sold by subscription tier. Let the plan lapse and historical data can become unreachable. Payment processing is mandatory, priced into the hardware discount. And the vendor's own public filings describe the other half of the bargain: transaction data aggregated across the merchant base feeds benchmarking products, platform development, and lending decisions. The operator's data is working around the clock, just not only for the operator. (Toast SEC filings; industry pricing analyses, 2026)

Delivery platforms are the clearest case, because it went to court. A restaurant fulfills the order; the platform keeps the customer, and passes along a first name, a last initial, and the items ordered. New York City passed a law in July 2021 requiring platforms to share customer names, addresses, emails, and phone numbers with the restaurants doing the cooking. The platforms sued. On August 5, 2026, the Second Circuit struck the law down as unconstitutional compelled speech. (2d Cir., Aug. 5, 2026; Reuters) The legal position is now explicit: the diner who ordered your food is the platform’s data asset, and the Constitution protects the platform’s right to keep it that way.

Two moves repeat across every version of this story. First, you cannot get your data out, or you pay by the month for the privilege. Second, your data goes to work in aggregate: benchmarks sold back to the industry, underwriting models, product development, all built from the operating truth of businesses that see none of the return. The value your operation creates accrues to someone else's platform.

The position we build from

Signals inverts the premise. We are a processor, not a custodian: the platform reads your operation, computes on site, and pushes every result to storage you control. Your data trains your deployment, and only yours; the sole thing that ever informs the broader model is anonymized pattern data, with nothing individual and nothing attributable in it. There are no data tiers, no export fees, and no aggregate products built on your numbers. If YYZdata disappeared tomorrow, everything your operation produced would still be sitting in the building that produced it.

Own your own data is four words, and every vendor will claim them. Two questions sort the market: can I have all of it, and what does it do for you when I am not looking.