# How Companies Can Use Big Data As A Strategic Asset

By **Gary Weinstein and Hudson Peters** (April 15, 2024)

Gary Weinstein

Hudson Peters

Everyone knows that machine learning and artificial intelligence is "The Big Thing," permeating virtually all aspects of our economy.

The most sophisticated organizations have not only developed proprietary AI technologies, but they have been using their AI technologies for many years — even before ChatGPT and other generative AI platforms burst onto the scene.

Now, many other organizations are trying to shift into high gear, attempting to figure out and implement their AI strategies. But most organizations are stuck in second gear — knowing that AI is a critical part of the future, but not quite knowing what this entails and how to get from here to there.

And in the meantime, almost everyone — apart from the most sophisticated companies — is engaging in a systemic failure to treat their big data sets as strategic assets to be protected and monetized. Although AI might be the engine to drive future business, big data sets are the high-octane fuel that powers AI.

There is an old joke about a man who worked in a factory. At the end of each day, he would go through the security check with a wheelbarrow full of trash. And every day the security guard would inspect his trash to make sure he was not stealing anything, but the guard never found anything wrong. On the day the man retired, the guard turned to him and said, "I know that you've been up to something for years. Now that you are retiring, please let me know what." To which the man replied, "It's true — I've been stealing wheelbarrows."

If only it were as simple as ensuring that others do not steal your big data. The reality, however, is that Big Tech does not need to steal big data sets because their customers readily hand them over without imposing any meaningful contractual restrictions on how their data may be used.

**What are big data sets and why are they important?**

Step back for a moment and think about your business.

You have data about so much — in fact, you have data about virtually every aspect of your business. Your key customers, how much they buy from you, your success rate at selling them new offerings, and how much of a discount you need to offer to make a sale.

Your manufacturing operations, including the cost of materials, cost of manufacture, cycle times, rates and types of manufacturing defects, and profit margins. The list goes on and on.

Your big data, if properly leveraged, can give you significant competitive advantages — and if improperly protected, this same information can give your competitors similar advantages, or at the very least they can undermine your advantages.

Many AI technologies, at their essence, involve one or more of the following:

- Creation: Creating complex tools to allow machines to "think," or more precisely, make sophisticated decisions quickly based on key data — and often a large amount of data.
- Discovery: Feeding those tools enormous amounts of data, and allowing the tools to look for interesting patterns and to learn ways to do something with those identified patterns, such as making business decisions and running business operations quicker, cheaper and easier.
- Improvement: Using those learnings to further improve the tool.
- Use: Running the tool on a company's day-to-day operating data to do something useful.

The biggest buzz from the onslaught of ChatGPT and other generative AI tools was producing content, including presentations, papers, agreements, briefs and memos. But AI is much more.

Imagine, instead, that AI is being used to help you make business decisions, or perhaps even make those business decisions automatically in a flash of a second, and also to help run your operations more efficiently.

This may include things like which products and services to manufacture; what price points to offer; which sales prospects should you pursue; how to save money in manufacturing; and which stock keeping units and components are susceptible to defects. All this, and more — and all based on information gleaned from your own company's big data.

And now, imagine that your key competitors are using your big data to make decisions about their businesses. And in doing so, they outflank you at every turn.

**But don't our contracts protect us?**

Over the past few decades, people started hearing about — and then sometime later started worrying about — data breaches.

As the breaches got bigger, and the associated damages — both monetary and reputational — got larger, people really started to pay attention, including the C-suite, and including the attorneys negotiating information technology contracts.

Customers began performing due diligence on their vendors, and often demanding audits, testing, certifications and strong contract protections. Data privacy laws and regulations were enacted, and IT contracts grew to include ever more robust data privacy and security provisions.

Early on, customers started including provisions in their IT contracts prohibiting their vendors from using any of the customers' personally identifiable information, or PII, in any manner other than to provide the requested services. Vendors often acquiesced, to a large degree, as long as they could use their customers' data with all of the PII removed and/or in an aggregated form.

The vendors were happy, particularly when the world moved from software installed on customers' on-premises computer systems to a software-as-a-service model, in which vendors held a copy of all of their customers' data. And customers, naively as it turns out, were happy too. After all, they had succeeded in getting their vendors to accept contract restrictions regarding data privacy and security and prohibitions on the vendors' use of PII.

But even without any PII, your data — and the learnings gleaned from your data and then implemented in an AI platform — contain huge amounts of information about your business, and vendors have been given a green light to incorporate this big data into their AI platforms. This makes their AI platforms more useful to their other customers, allowing them to grow market share and/or raise their prices.

### Who's minding the factory?

These changes do not happen in a vacuum, of course. At some point along the way, when negotiating an IT contract, one of the customers' attorneys — who of course is familiar with the wheelbarrow joke — realizes what has been going on.

She alerts her client to the fact that they have this strategic asset, namely their big data, and they are giving it to the vendor with full permission to use it in any and every way, so long as the PII is removed. The client acknowledges this risk and instructs the attorney to push back. The attorney tells the vendor that they cannot use the customer's data other than to provide the vendor's SaaS system, even if the PII is removed, and even in an aggregated form.

But then the vendor digs in, saying that their system does not allow for restrictions on non-PII aspects of customer data, or saying that they are only able to offer their relatively low prices because of the broad permission to use non-PII aspects of the customer's data.

What happens next? Well, far more often than not, the key decision-makers for the customer care mostly about the following:

- Does the software solution provide the desired functionality?

- Is the software solution reliable?

- Does the software solution have adequate cybersecurity?

- Is the software solution user-friendly?

- Can the software solution purchase and implementation project be completed within the allotted time?

- Can the software purchase solution and implementation project be completed within the allotted budget?

Missing from this list is any notion of protecting the customer's big data sets as strategic assets. So even when a customer's attorney pushes their key decision-makers to fight for restrictions on the vendor using non-PII aspects of customer data, such restrictions are almost always a low priority for the customer's IT stakeholders and procurement team responsible for selecting and implementing the software solution.

In an ideal world, the company would have a senior leader tasked with treating the company's data as a strategic asset, and for promulgating processes and procedures to ensure that the company does so — including in contract negotiations.

Unfortunately, all too often the chief technology officer's or chief information officer's plate does not have much capacity to focus on big data in the context of IT contract negotiations because their plate is too full worrying about the reliability of IT systems, cybersecurity, compliance with regulatory requirements particularly related to privacy and security, help desk support, systems planning, budgeting, overall strategic vision, and all of the other critically important functions of running an IT department.

Turning back to those contract negotiations. When the vendor rejects any restrictions on non-PII aspects of customer data, or says that adding those restrictions will delay the project significantly or will cost the customer far more money, there is nobody at the company who is empowered and responsible for pushing back. And so customers concede the issue, time and time again.

**What can you do?**

First and foremost, companies and other organizations should shift their mindset and begin thinking about their big data as a strategic asset. This includes appointing a senior person with the responsibility and the authority to make sure that this shift happens.

Second, when conducting a request for proposal for a new IT system, issues regarding big data should be treated with the importance they deserve — right up there with all of the key technical, functional and budgetary requirements — rather than an afterthought left to be handled in contract negotiations after the vendor selection has already been made.

To this end, the RFP evaluation team must understand their company's needs and policies with respect to big data before making any tentative selections.

Third, they should be prepared to roll up their sleeves and think hard about the different types of data the applicable IT system uses, touches, creates and stores — and then divvy up the data rights.

**Divvy up the rights to the data.**

It is human nature, or at least the first instinct of attorneys, to approach things from the perspective of "I own this stuff, and you own that stuff." When talking about tangible assets that approach often makes sense.

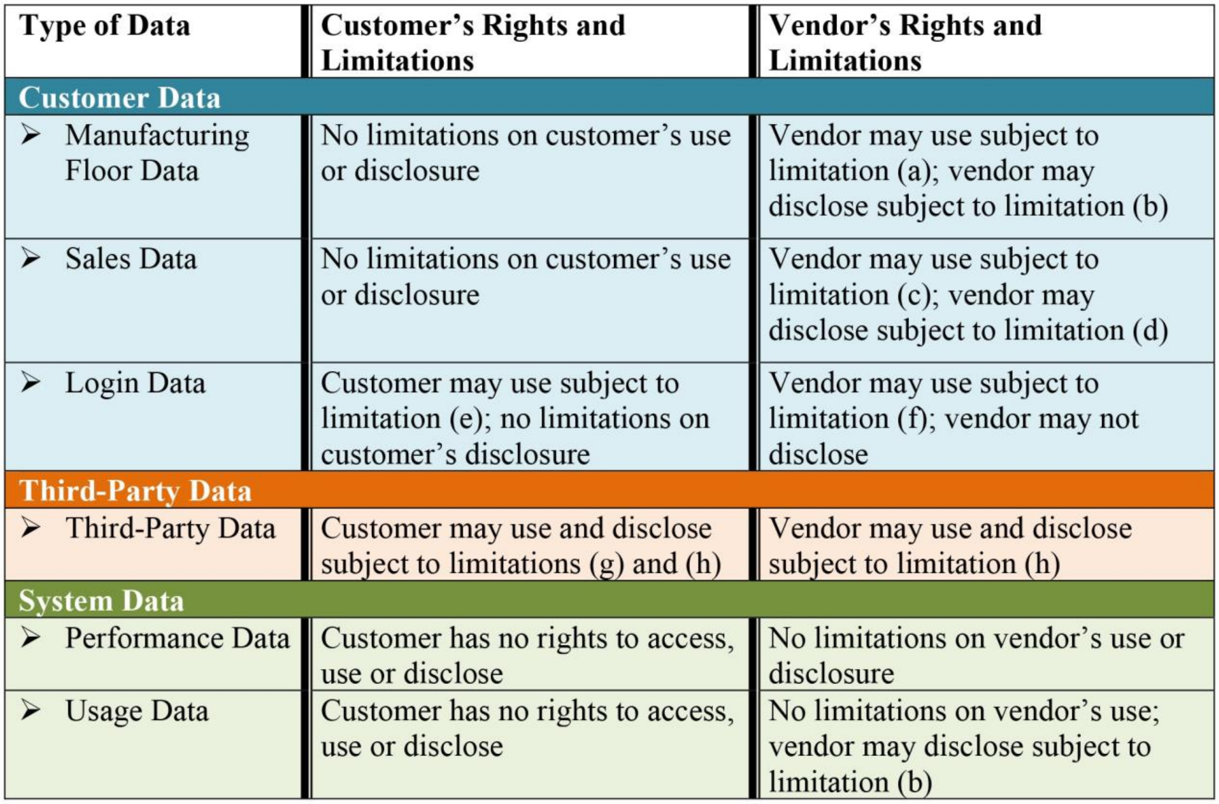
But with respect to intellectual property rights in general, and data in particular, things are often far more nuanced, and focusing on ownership can distract from the more important question of what each party may and may not do with the data, regardless of who owns it.

We instead recommend the following approach.

First, conceptually break the available data down into some big buckets, such as system data, third-party data and customer data. Then break each of those buckets down a bit further until you arrive at clearly defined discrete groupings for which all elements thereof can be treated alike.

Second, for each group, outline what specific things each party is and is not allowed to do with respect to that type of data in its original form, in a form that identifies PII, in a form that identifies both PII and all relationships with the customer, and in a fully aggregated form. All while avoiding words based on "own" or "ownership."

Here is a partial sample of how to approach this topic:



| Type of Data | Customer's Rights and Limitations | Vendor's Rights and Limitations |
|---|---|---|
| **Customer Data** | | |
| ➢ Manufacturing Floor Data | No limitations on customer's use or disclosure | Vendor may use subject to limitation (a); vendor may disclose subject to limitation (b) |
| ➢ Sales Data | No limitations on customer's use or disclosure | Vendor may use subject to limitation (c); vendor may disclose subject to limitation (d) |
| ➢ Login Data | Customer may use subject to limitation (e); no limitations on customer's disclosure | Vendor may use subject to limitation (f); vendor may not disclose |
| **Third-Party Data** | | |
| ➢ Third-Party Data | Customer may use and disclose subject to limitations (g) and (h) | Vendor may use and disclose subject to limitation (h) |
| **System Data** | | |
| ➢ Performance Data | Customer has no rights to access, use or disclose | No limitations on vendor's use or disclosure |
| ➢ Usage Data | Customer has no rights to access, use or disclose | No limitations on vendor's use; vendor may disclose subject to limitation (b) |

**Final Thoughts**

Like the security guard at the factory, it is important to understand the value of all of the items your business owns and creates, including your data.

Without fully identifying the worth of your data and treating it as a financial asset — rather than merely a security issue and a regulatory compliance issue — during the course of vendor selection and contract negotiations, you risk destroying your big data as a strategic asset and enabling your competitors. And at the very least you are giving your vendors lucrative usage rights without getting properly compensated.

This is particularly true as AI technology has increased the importance of big data sets as strategic assets. Fortunately, this is an imminently fixable issue, with some forethought and investment by your organization.

Ultimately, AI technology powered by big data has the potential to create radical improvements to business operations — the question is whose business your big data will be powering: your vendors' and competitors', or yours.

---

*Gary S. Weinstein is a partner and Hudson W. Peters is an associate at Faegre Drinker Biddle & Reath LLP.*

*The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.*