

The data-driven supply chain raises new governance and security issues

BY SHAWN MUMA, DAVID KAPPOS AND CARYS WEBB

With every business now a data business, good data stewardship is a must.

Over a century ago, companies transitioned to making ubiquitous use of electricity, helping to usher in the Second Industrial Revolution with innovations that made it easier to mass produce goods and transform the way we work and live. Today, companies are transforming their operations to make ubiquitous use of data. The digital transformation of businesses has brought the global economy to where every enterprise—large or small—is a “data enterprise.” A company may be a hospital, or it may be a Tier 2 supplier of auto parts, but no matter what its operations are, it must think of itself as a “data-driven company,” regardless of the products or services it provides to its customers or clients.

Business leaders need to consider the question: Is my organization ready for the future as a data enterprise? Many companies have already taken steps in recognition of their reliance on and usage of data, and its importance to their businesses. But the goalposts are continuously moving. Practices that were adequate in the past are proving inadequate in our fast-evolving global economy and regulatory environment. Even companies making concerted efforts can find they come up short, with potentially dire consequences.

Nowhere is the need for a new understanding of the role of data management more pressing—and challenging—than the transformation to a digital supply chain underway in every industry, in every market. As enterprises move to digitally integrated supply chains and increasingly link customer, demand, and supplier data to optimize business workflow, the use of data and data security is of critical importance. Good data stewardship is now expected by customers and suppliers alike. Enterprises need to find ways to embed data governance and security in their operations both internally and with third parties, including their partners, suppliers, and distributors. It must become part of the culture.

Shawn Muma is director of supply chain innovation and emerging technologies for the Digital Supply Chain Institute (DSCI), a non-profit initiative of the Center for Global Enterprise. His experience includes structuring and managing technology alliances for IBM in the U.S., Europe, Asia, Middle East, and South America in a wide variety of industries including aerospace and defense, investment banking, retail banking, chemical and public sector. You can reach Shawn at smuma@thecege.net.



David Kappos is a partner at Cravath, Swaine & Moore LLP and former director of the U.S. Patent and Trademark Office. Prior to leading the USPTO, Mr. Kappos held several executive posts in the legal department of IBM where he served from 2003 to 2009 as vice president and assistant general counsel for intellectual property.

Carys Webb, CIPP/US, is an associate at Cravath, Swaine & Moore.

Accelerating this need is the move from the traditional supply and sales channel to business processes that extend beyond enterprise boundaries toward so-called “supply chain constellations.” Instead of adhering to the rigid, linear supply chains of the past, individual enterprises can have a role in numerous “constellations” based on varying activities to better serve the needs of others in the supply chain and, ultimately, consumers. The ubiquitous sharing of data makes these constellations powerful tools that touch every enterprise process and beyond.

Considering this fast-evolving digital landscape, how do companies share data in a supply chain constellation? How do they determine what data can be shared, with whom, and identify, implement, and manage applicable use restrictions? How do enterprises develop robust data-sharing governance policies? Businesses should think about data stewardship through three lenses which we have labeled below as Category I–III for ease of discussion:

Category I. Confidential or proprietary data that provides a business with competitive advantage such as unit cost, product design information or projected sales volumes.

Category II. Personally identifiable information (PII) about customers, employees, and suppliers that is increasingly subject to statutory and regulatory requirements.

Category III. Specific-use data that can be shared for business optimization without fear of competitive exposure; for example, available space within a container to optimize shipping cost. Generally, this data is shared amongst a closed cohort that may include partners and even competitors with aligned interests.

Each of these categories requires different data governance and protection. Of course, data travels in both directions—thus, an enterprise is both an owner of data and a user of others’ data. Governance and security policies must consider both.

Engaging in this analysis will help businesses move away from traditional supply and sales channels toward supply chain constellations. This article aims to provide guidance by identifying actions enterprises should take and offers practical guidance for implementing comprehensive data-sharing policies to become a good data steward. We chart a course for

process evolution enabling every data business—and as such, every business—to bolster its data-sharing policies and security standards.

Considerations for good data practices

1. Why is data being shared?

This is the fundamental question. Information can be shared across a supply chain constellation for several reasons, including sensing and stimulating demand, predicting arrival time of product at a distribution center, or managing ESG (environment, social, and governance) objectives.

Category I data that provides a competitive advantage should be tightly controlled and reviewed at senior levels within a company before it is made available to trusted suppliers. Technology must be implemented that controls access and provides an audit trail. Ownership of the data must be clearly maintained and use restrictions identified and made legally binding. If you are an athletic apparel manufacturer, you do not want your supplier sharing your shoe design with your competitor who may also be a customer of that supplier.

For Category II data, enterprises should check their privacy notices for whether the purpose for sharing data has been transparently and accurately disclosed to consumers. Privacy laws may restrict a company’s ability to share data for a new purpose not previously specified in its privacy notice. The European Union’s General Data Protection Regulation (GDPR), for example, only allows personal data to be shared for a new purpose if one of the following conditions is met: (i) the new purpose is compatible with the original purpose; (ii) the company obtains consent; or (iii) the company has a clear legal obligation. These privacy laws, however, may not consider anonymized, de-identified or aggregated data to constitute personal data. If a company’s privacy notice provides for anonymization of personal data, then the company may be able to share the anonymized (now non-personal) data for purposes not previously specified in its privacy notice. If not provided for already, companies should consider providing in their privacy notices for the anonymization of personal data and the use of de-identified or aggregated personal data.

Category III data can be openly shared across a supply chain constellation but must be shared in a

manner consistent with its intended use. Even though the data is made available to interested parties for a specific use, the owner still must ensure the data is being used as intended and any regulatory or contractual restrictions are complied with—for example, sharing data only as permitted by confidentiality restrictions or within applicable geographic limits.

2. What (type of) data is being shared?

Digital supply chains are premised on receiving and sharing data in concert with suppliers through multiple tiers, distributors, partners, and customers, all ideally in real time, and including status reporting, feedback, data analysis and decision support/recommendations. Visibility and auditability into the status, performance and requirements of all parties is now essential to enterprises predicting and responding to issues efficiently. This makes the what of digital supply chain data management a threshold-critical consideration.

Enterprises should carefully review (think audit) the types of data directly and indirectly received from any third party, including suppliers, distributors, and partners, and examine how such data is used, stored, and protected, ensuring compliance with any legal obligations. Data collected, received, used, and stored is data potentially shared.

As a subset of the data identified above, the company should understand how the data is intended to be used. Each data element within an entity should be handled by a responsible party to ensure the data is managed, stored, and used as intended by the data owner, which may be within an enterprise or external to the enterprise.

For Category I data, enterprises in their digital transformation journeys are installing sensors, radio frequency identification (RFID) tags, GPS trackers and the like to monitor manufacturing, packaging, inventory, shipping, and delivery status, among other factors. Sharing such information with others in their supply chain constellation raises rights-of-use as well as confidentiality issues. Both should be managed with intentionality, to provide the appropriate use-rights—but not more rights than are needed—and to ensure appropriate confidentiality treatment for applicable information. Moreover, consideration should be given to not sharing information that is particularly sensitive, or which does not add much/any value beyond other information being shared. For

example, information concerning the completion of manufacturing or packaging, may be more appropriately shared outside a company compared to detailed data that can reveal more sensitive internal secrets, such as pricing strategies or vendor lists. Key trade secrets and proprietary algorithms, and the data driving them, likely should not be shared on any terms.

Category II data—both data that is PII generally (like email addresses and tax ID numbers), and data that may inferentially constitute PII (such as prescription medicines ordered by an identified individual) requires special identification and attention as both can be PII regulated by privacy laws such as the California Privacy Rights Act (CPRA) and GDPR.

Similarly, as for Category I data, use rights should be appropriately considered for Category III data as it is shared with those within a constellation for a limited purpose but is not accessible by those outside of the defined ecosystem. All shared data should be subject to applicable data integrity and security measures, including the Payment Card Industry Data Security Standard (PCI DSS) for any credit card information. While the sharing of PII and proprietary data may be restricted, enterprises in a digital supply chain should actively seek out opportunities to share information that can create a stronger supply chain constellation, whether that information involves sensor data, permitted customer information, or current threats and security best practices.

3. With whom is data being shared?

Digital supply chain data can be shared internally across functions, as well as externally across distributors, suppliers, partners, customers and other third parties in a supply chain constellation. One should ask why does this individual or entity need this data? For what purpose? How will they use it? Who will have access to it? Can it be shared with others? How will it be protected? Will such protection comply with how the sharing enterprise expects that data to be protected, and how will the sharing enterprise be assured of its protection? Data repositories, where companies typically centralize the storage of critical enterprise information, are behind and playing catch-up in their ability to manage rights-of-use characteristics.

For data that is confidential or proprietary, most businesses have well-defined internal information protection procedures; however, as that information is

increasingly shared beyond the enterprise walls in support of supply chain transparency and customer demand planning, there needs to be (contractual, technical and compliance) assurance the data is protected in a manner that is consistent with corporate policies. Technology such as blockchain can manage data access and workflow across a constellation of connected enterprises and ensure compliance with contractually defined policies. For example, rather than relying on a series of intermediaries to share data between two parties, data sharing can be accomplished using smart contracts. These smart contracts will autonomously run what they are programmed to run—meaning contractually defined policies for data sharing can be written in code. This provides technological rigor to enforce such policies, rather than relying on intermediaries' compliance.

A similar understanding of how data is being used and who has access is necessary for all shared data, even that which is not sensitive. Not only is it good stewardship, but future data protection regulations will likely require active data management for all shared data. Developing good practices today will ease the burden of future compliance.

Internally, PII and confidential information shared among employees may need to be protected and limited on a need-to-know basis through access control mechanisms. Employees with access to confidential or trade secret information may need to sign confidentiality or non-disclosure agreements. In a digital world, these controls need to extend beyond the traditional enterprise boundary.

Externally, data sharing may be subject to different requirements based on how the entity with which data is being shared is classified under privacy laws. For example, the CPRA recognizes entities as a covered business, service provider, contractor or third party, and the GDPR classifies entities into independent or joint data controllers, processors and third parties such as sub-processors.

Data protection obligations may be heightened when sharing information with third parties. If a business shares personal information with a third party, this data sharing may require prior written authorization from a data controller under the GDPR or constitute “selling” or “sharing” personal information as broadly defined by the CPRA, leading to additional requirements such as

placing a “do not sell or share my personal information” link on the business' homepage and allowing consumers to exercise their right to opt out.

If a business shares personal information with a service provider or a contractor under contract, on the other hand, this data sharing may simply be considered “disclosing personal information for a business purpose” under the CPRA. The business is still obligated to inform customers of the categories of personal information being disclosed for business purposes in the business's Privacy Policy, but the business will not be obligated to offer consumers the right to opt out or be required to comply with certain other requirements triggered by selling data.

4. From where and to where is data being shared?

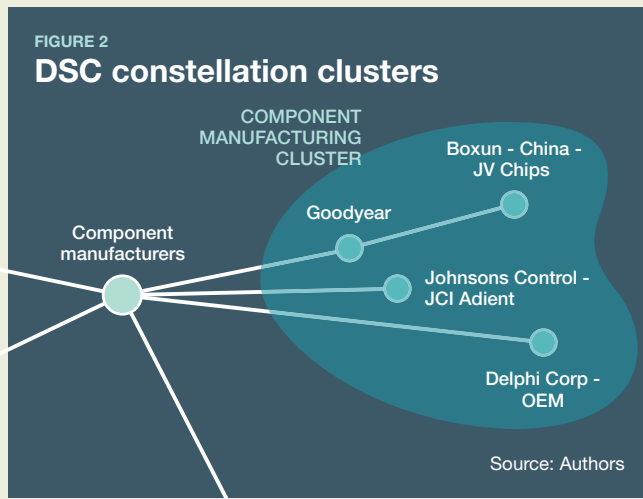
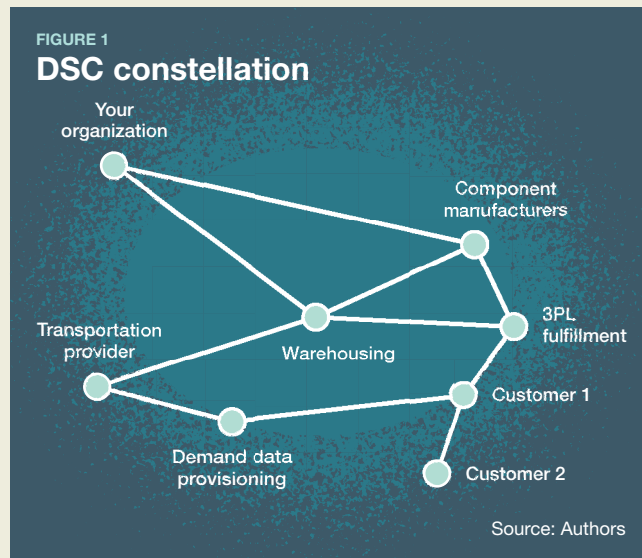
Companies sharing (sending) data outside of their home jurisdictions (e.g., to their customers or suppliers located in different geographies) should be mindful of the laws and regulations of the jurisdictions to which they are transferring data; for example, GDPR regulates countries where certain PII can be stored. This is increasingly important as data is shared with suppliers that may be in non-approved countries or where a cloud provider may operate and store business data. Some countries, such as Malaysia, have data controls that rival those of the EU or California. Consideration must also be given to where data backups are kept. Indonesia, for example, does not allow banks to back up data in other countries such as Singapore, which would by most standards be considered secure.

For digital supply chains spanning the Atlantic, transfer of personal data from the European Union or United Kingdom to the United States may require special attention. Such transfers are not clearly permitted under any law, and minimally require mechanisms like standard contractual clauses (SCC) described in the GDPR.

If data is coming from customers, monitoring such data through data-field limitations (i.e., providing no opportunity for the customer to provide certain PII), filtering, manual review or artificial intelligence may help enterprises prevent sensitive information from being inappropriately uploaded to their systems. For example, while a company may prohibit customers from providing credit card information, users may provide this data at their own instance, such as by a user

Digital supply chain: It's moving from linear connections to "constellations of value"

Even though we still refer to the supply chain when we are focusing on the operational efforts to bring products and services to customers, most advanced supply chain leaders more likely think of a "constellation of value," that is, clusters that form constellations of suppliers, suppliers to suppliers, manufacturing and service partners, and logistics service providers. Rarely is the process a simple linear connection between upstream and downstream partners. It is more like a three-dimensional network, a 3D constellation map of value partner's operations as you can see in the following two charts.



Connecting the nodes in a constellation orchestrating them into a high-performance digital supply chain often requires complex negotiations and relationships and sharing critical pieces of data and information inside and outside the organization. The FSF digital supply chain integrates these orchestrated collections of partners to meet customer needs effectively. Bringing together the elements of these value chains is not always easy, but the business benefits of successful integration have the potential to activate new, competitively advantaged, business models that are hard to replicate. Being hard to replicate create the opportunity for firms to grow their businesses while managing costs.

placing a picture of their credit card in a free form image submission field. Manual review of certain fields may be required to ensure such data is removed from the company's system.

In digitally-connected supplier constellations, well-defined data governance and security that extends beyond the enterprise is essential to maintain competitive advantage and achieve contractual and regulatory compliance.

Survey of the regulatory landscape

It is important to understand what is required by current laws and regulations. Statutory and regulatory requirements must be demonstrably met in an increasingly complex and ever-changing environment. A company's obligations will be dependent on the countries/states in which the company does business, as well as the countries/states of residence of the people whose personal information it holds or processes.

Companies holding or processing data from individuals in the European Union or United Kingdom have long been subject to the GDPR and its UK equivalent. More recently, in late 2021, the Personal Information Protection Law came into effect in China.

The United States generally takes a sectoral approach to data privacy and protection. Federal laws and regulations cover areas including children's personal information, electronic health care transactions, credit report information and financial institutions, as primarily enforced by the Federal Trade Commission (FTC).

On the state level, five U.S. states have enacted comprehensive data privacy laws that are primarily enforced by state attorneys general, and several other states have privacy laws in committee. Notably, California has had a comprehensive data privacy law in effect since 2020. Both the California attorney general and the recently established California Privacy Protection Agency (CPPA) have enforcement authority.

Next, enterprises should understand that the landscape is ever-changing, and should continuously address emerging regulations. The best thing companies can do is to closely follow trends and best practices, quickly implementing those that are applicable. Demonstrating that reasonable steps have been taken


to achieve and retain compliance with laws and regulations will go a long way with regulators in the event of an investigation or a cyber-intrusion that requires self-reporting to regulators.

A growing number of U.S. state data privacy laws have gone into effect this year, with Utah set to join the list on Dec. 31 when its Utah Consumer Privacy Act goes into effect. Laws went into effect in California (California Privacy Rights Act) and Virginia (Virginia Consumer Data Protection Act) on Jan. 1 of this year and Colorado (Colorado Consumer Protection Act) and Connecticut (Connecticut Data Privacy Act) added laws effective on July 1.

The next three years will see additional states add laws, including Oregon (Oregon Consumer Privacy Act) and Texas (Texas Data Privacy and Security Act) on July 1, 2024, and Montana (Montana Consumer Data Protection Act) on Oct. 1, 2024. Following that, Iowa (Iowa Consumer Data Protection Act) on Jan. 1, 2025, and Tennessee (Tennessee Information Protection Act) on July 1, 2025, will add laws and Indiana (Indiana Consumer Data Protection Act) is slated to enact its law on Jan. 1, 2026.

Even more states have enacted data privacy laws, and more progress through the state legislative process. Companies in these states or falling under the extraterritorial reach of these state laws (e.g., by doing business with individuals or entities in these states) should update their privacy policies and practices.

Conclusion

This article focuses on digital supply chains as an environment where the need for action to deal with data ubiquity is pressing. But digital supply chains are just the beginning. All aspects of business touch on data and require cognizance of applicable issues. Data governance, privacy and security must be actively managed from the top of the enterprise. Good data stewardship is increasingly a reflection of brand values and a customer expectation. 

This article is for general information purposes and is not intended to be and should not be taken as legal advice.