Bloomberg Law

Professional Perspective

Protecting Supply Chain Data

Ronald M. Leibman and Morgan Jones, McCarter & English

Protecting Supply Chain Data

Contributed by Ronald M. Leibman and Morgan Jones, McCarter & English

Advancements in digital freight management, visibility tools, network solutions, and data amalgamation have given the supply chain industry the ability to obtain, share, and analyze shipping and other logistical data with increased ease and speed. These tools and today's more sophisticated digital marketplaces present lawyers with some difficult questions.

The first question is rooted in a fundamental concept that predates our current high-tech world: how to protect an organization's proprietary information from falling into the wrong hands. The second question is relatively new and evolving: whether the data a company collects and shares includes personal records covered by the ever-increasing regulatory framework for such information.

Contractual Protections

With regard to the first question, the nondisclosure agreement or a confidentiality clause in a final contract remain foundational data-protection tools. In either case, the starting point must be to determine what company data constitutes "confidential information" for its proposed use; in the context of logistics, this data typically includes rates and charges, customer lists, lane volumes, facility throughput, and other industry-specific information.

Today, though, these items alone may not be enough—a discloser needs to review not only the data it has provided to another party, but also what that party may derive from that information. For example, disclosure to a tech-enabled entity of destination addresses without the customer name may not be sufficient to keep the customer's identity private. Other issues include protection of third-party data for which the discloser has a freestanding confidentiality agreement and, however unlikely, whether confidential information only includes data marked as "confidential."

While the use of an NDA or a contractual confidentiality provision may seem like first-year law school contracting, in today's world, where tech suppliers seem to have a leg up on their customers, data protection is sometimes lost in the supplier's form agreements. An example is found in a logistics/transportation software provider's "Software as a Service," or SaaS, agreement, recently presented to a client. The pact's confidentiality section defined "confidential information" in a way that initially appeared to be suitably broad, with obligations that applied mutually to both parties, along with a nondisclosure requirement.

Upon closer scrutiny, however, it proved to be lacking, as the confidentiality section imposed no specified limited use covenant on the receiving party. This means the software provider could use the client's confidential information for uses beyond those necessary to meet its contractual obligations as per the client's expectations. The nondisclosure obligations also allowed the vendor to disclose the client's confidential information to its employees, agents, and advisers who have a "need to know" and who are bound by confidentiality obligations.

Normally, a need to know is attached to a use limitation. Here, without such clarifying language, the receiver arguably had no such limitation and could theoretically, in compliance with this agreement, disclose our client's confidential information to its employees for its own purposes. Finally, this agreement did not require the return or destruction of the client's confidential information either during or after the expiration or termination of the agreement. This, in combination with the lack of a use limitation, could cause the client to lose control of its confidential information forever. Given the noticeable missing elements in this confidentiality section, the vendor arguably could use the client's confidential information to compete with the client without legally violating this aspect of the agreement.

Confidentiality and Publicity Rights

In addition to NDAs and contractual confidentiality provisions, many data-driven companies add confidentiality terms to their purchase orders, invoices, receipts, and other commonly used documents that are often used separately from, and at times in place of, more formal agreements. Generally, these documents favor the party who drafted them, and may seek to override terms from previously negotiated formal agreements. To avoid these situations, it is important that there be a legal review of any documents involving information sharing, and that previously agreed to formal confidentiality provisions be attached to any subsequent documents.

Closely related to the concept of data confidentiality is the matter of limited publicity rights. The two subjects may at times need to be considered concurrently because a publicity rights section may extend beyond the agreed limitation of having one company use another company's name. If combined with a confidentiality provision that fails to state that data use should be permitted expressly for specific contractual purposes, the result is a publicity clause that is not restricted to simply posting the client's name as an entity using the vendor's SaaS solution; in fact, the vendor would be able to post any confidential information disclosed by the client.

This is sometimes seen when data indexers/aggregators publish "aggregated" and/or "anonymous" information to the shipper and carrier public. To safeguard against this potentially damaging disclosure, companies should seek to ensure their sensitive logistics data is subject to restrictions, such as data sets having a certain minimum size, and by taking the necessary legal steps that would prevent the linking of the proprietary information they provided to the disclosing party, its suppliers, or its customers.

Statutes and Regulations

As highlighted by the applicability of traditional contractual data-use restrictions, the idea that confidential information needs to be protected from unwanted distribution is not new and, not surprisingly, has some statutory protections under certain logistics statutes, such as Title 49. While quaint by today's standards, especially given the breadth of data traded in the current supply chain ecosystem, both 49 U.S.C.14908 (for motor carriers and brokers) and 49 U.S.C. 11904 (for railroads), in certain circumstances, prohibit modal or broker entities from disclosing shipping and routing information. It is notable that these statutes do not extend to other entities that may obtain such data, which today would include tech-enabled services, or perhaps even digitally engaged factoring companies. Additional statutes regarding the protection of personal data that can impact the supply chain industry have emerged over the past few years, most notably the European Union's General Data Protection Regulation and the California Consumer Privacy Act.

Both the GDPR and the CCPA apply to data that identifies individuals, not companies. As a result, the statutes are addressed in a section separate from other confidential information in most agreements. Importantly, these laws are extraterritorial, meaning they can be applied to the actions of entities outside of the jurisdiction that created them. This is critical to supply chain data protection since what may appear to be a purely business-to-business transaction may in fact involve the dissemination and protection of personal information, such as information relating to last-mile delivery.

The CCPA protects the personal information of California residents. It provides them certain rights with regard to their data, while imposing obligations on companies in or outside of California that hold such data and have at least $25 million in global revenue per year, buy/receive/share/sell the personal information of 50,000 or more California residents per year, or derive at least 50% of annual revenue from the sale of California resident information.

The statutory definition of personal information is broad, going beyond the usual categories such as name, email, phone number, Social Security number, and driver's license number. It also includes biometric, internet activity, geolocation/GPS, audiovisual, and employment-related information. This means, for example, where a shipper, carrier, broker, or tech-enabled third-party uses GPS tracking of a shipment, and the driver resides in California, the CCPA will potentially be implicated by the collection of the resulting data.

Still, the activities discussed above are not violative of CCPA provided the requirements of the law are met. These include providing the driver a specific notice at, or before, the point of collection; updating the company's privacy policy to statutorily required language; and deleting the driver's information upon his or her request. The latter two obligations likely pose the greatest obstacle for tech-forward logistics companies, but are softened by certain exceptions to the data-deletion requirement, including completion of the transaction that prompted the collection of the data, certain internal uses, and compliance with a legal obligation.

That said, there is no exception should the driver request that his or her information not be sold. This obligation is further complicated by the statute's broad definition of "selling," which includes virtually any activity whereby one party provides the personal information of a California resident for money or for any other valuable consideration. This could include, for example, a vendor reserving the ability to use data that its customer has provided, or collecting data for other purposes that might provide the vendor with another stream of revenue in exchange for providing a reduction in the price of services to the disclosing company.

While the CCPA may be the big fish in the U.S., supply chain entities operating on the other side of the pond should familiarize themselves with the GDPR. This 2018 EU law applies not only to EU-based companies, but also to companies outside of the EU that offer goods and/or services to, or that monitor the behavior of, people in the EU (also referred to as "data subjects") and the processing of the personal data of such persons. Here, processing means virtually any activity including, but not limited to, data storage. And, as in the CCPA, personal data is deliberately defined broadly. In order to lawfully process data that is subject to GDPR, there must be a "lawful basis" to do so, which can include, the consent of the data subject, the completion of a contract with the data subject, compliance with a legal obligation, or for the company that decides the particulars of processing the data, often referred to as "controllers."

Many controllers proceed on consent, as it is a more efficient and cost-conscious approach compared to other methods. The drawback to consent, however, is that it can be withdrawn. While other lawful bases also have their set of pros and cons, many believe that the more effort spent in establishing these at the outset, the tougher it will be to invalidate. Having other legal bases can allow the controller to continue processing personal information even after the data subject withdraws its consent. Still, this approach would remain subject to a data subject's rights under the GDPR in addition to the controller's other obligations, including mandatory agreements with service providers that process personal data for the controller.

The GDPR also includes the concept of the onward transfer of data, which permits the transfer of data outside of the EU (and/or other countries) that the EU deems as providing adequate data protection. This is triggered when an international company conveys data to a central database, its global headquarters or to processors. If a company is transferring data in this manner, extra steps are required to in order to avoid fines, which can start at €20 million.

Even if the CCPA and the GDPR do not apply to an individual or class of supply chain players today, new data privacy laws are frequently being proposed in the U.S. and overseas, with the two statutes serving as useful blueprints. CCPA and GDPR notwithstanding, corporate clients should consider adopting certain specific measures that are likely to apply to any set of data privacy laws: taking data inventories, or "mapping data," establishing processes to receive and respond to requests from a data subject, and forging agreements with business partners to control the uses of personal data.

Conclusion

From all indications, supply chain technologies that ferret out operational and other supply chain data will only increase in use, scope, and functionality as industry professionals seek ways to maximize efficiency and minimize cost. Yet, the technology that makes data extraction and transmission easier, also carries the risk of a receiver using a provider's confidential information unlawfully or in a manner that is contrary to the provider's interests. For this reason, companies in the supply chain need to closely monitor the behavior of their counterparties in using and protecting their data. Using the advice of counsel, companies should seek to secure written agreements with strong nondisclosure policies to assure both the efficacy of these policies and compliance with applicable law.