Association of Technology Law Professionals

Permitting Vendor Use of Customer Data (It's Not About Data Privacy or Data Security)

Materials Accompanying February 11, 2022, Meeting

In a vendor-customer technology agreement, after addressing all of the state, national, and other data privacy and security requirements identifying what the vendor can't do with the customer's data, what's left? Well, what's left are the contract terms that actually permit certain vendor uses of the customer data. These terms, and the steps each contracting party can take to address today's new data concerns, have never been as important.

Change is Inevitable

Contractually addressing a technology vendor's right to use its customer's data, whether it's personally identifiable information or non-personal business data, has been in contract negotiation playbooks for decades. Among other concerns, attorneys and contract professionals have routinely sought to tackle issues related to ownership of and rights to use customer data, customer rights to provide data furnished to it by third parties, and the parties' obligations to manage risks and assume burdens associated with personal data. These concerns not only apply to data made available directly by the customer to the vendor, but to data generated by the vendor using the customer's data in the course of providing services.

Recent developments in the world of data, however, significantly change the negotiation playbook and how commercial terms in technology contracts should address data disclosure and use. For one, the explosion in the development and deployment of artificial intelligence products and services has placed new, incalculable value on data and its collection. AI software revenue worldwide in 2018 is expected to increase exponentially (to $126B) in the next three years. For another, the growing number and scope of U.S. state laws restricting the gathering and use of personal data is further limiting the quality and quantity of data available for commercial use. (Today, the full implementation of new data laws in California, Colorado, and Virginia will occur next year. Tomorrow, there will be others.) Separately, recent business announcements by the likes of Apple and Google, limiting the availability of user data to third parties, have also increased the premium on obtaining data from other sources. And, for customers sharing data with their vendors in a seemingly lawful way, even permitted vendor uses are coming under public scrutiny, and 34% of customers said they'd stop buying products and services from a company that is involved in a data incident. How do contracting parties deal with this change?

The Data Frame: Form of Contract

Nearly every negotiation of a technology contract involving customer disclosure and vendor use of data begins with a discussion of which party's form of contract will govern the relationship. There are countless considerations that weigh on this decision – many real, others not. However, with respect to data issues, the better the start, the faster and more efficient the finish.

Technology customers asked to negotiate from the vendor's form contract should assess the following before deciding how to proceed:

- Does the vendor form address, or ignore, statutory, regulatory, and other legal requirements that are unique to the customer?
- Does the vendor form require customer disclosure of more data than is needed for the vendor to provide the contracted products or services?
- Does the vendor form require customer disclosure for purposes other than just providing services to the customer?
- Is the vendor form based on the requirements and operation of the vendor's current data gathering and use systems, or does it contemplate a future, less-controlled state of the vendor's data collection processes?

On the other hand, technology vendors requested to start with the customer's paper should consider the following before agreeing to use the customer's form:

- Does the customer form provide the vendor with the full scope of data and rights the vendor needs to provide the contracted products and services?

- Does the customer form assume vendor system limitations on data gathering that the vendor cannot implement?
- Does the customer form impose data collection and use requirements on the vendor that are based on possible (and more restrictive) future laws or standards, rather than actual, current requirements?

The Data Front End: Introduction of Customer Data

It is rare when a customer and vendor cannot conclude a technology transaction because the customer cannot provide or agree on the minimum data needed for the vendor to provide the desired product or service. That said, given the variety of customer data sources and the evolving legal treatment of data rights, the customer should fully vet its ability to provide the data in question to the vendor.

Certainly, the customer should review all applicable state, national, and other data privacy and protection laws to determine whether it has the right to disclose relevant data to the vendor, as well as what restrictions may apply to the data. Moreover:

- If the customer will be providing data it received from third parties, the customer should evaluate the contract terms governing its rights to further disclose the third-party data. The customer should also review whether future changes to those terms may later restrict vendor receipt or use of that data in ways that, at the time of contracting between the customer and vendor, are otherwise permissible.
- When the customer may be disclosing employee data to the vendor, if the employees are under a collective bargaining agreement between the customer and the employees' union, the customer should carefully review that collective bargaining agreement.
- If the customer will be sharing data gathered from its website or other venues governed by online or other privacy policies, the customer should review those policies to determine what they allow.
- The customer may also want to consider impending changes in applicable data privacy and protection laws to see whether disclosures and uses that are presently permissible may soon be disallowed.

Despite agreed contract terms describing the scope of data to be provided by the customer, in implementing the contract it is not unusual for the customer to provide more data than the agreement contemplates or for the vendor to collect more than is permitted. To manage this risk, each party should investigate whether it can implement operational or technological measures to reduce the likelihood of over-disclosure or over-collection. In addition, in the technology agreement:

- The customer should consider contractually obligating the vendor to not request, collect, or access more data than is needed for the permitted purposes under the agreement.
- The customer can seek to require the vendor to immediately destroy or return all data as soon as it's no longer needed for the permitted vendor purposes.
- The customer should weigh obligating the vendor to not collect or gather any personally identifiable information unless that quality of information is strictly necessary for the vendor to perform under the contract. That is, anonymized, de-identified, pseudonymized, or aggregated data may be sufficient.
- The vendor should consider contractually requiring the customer to not provide or make available more data than is needed for the vendor to carry out the permitted purposes under the contract.
- The vendor could impose on the customer an obligation to not provide personally identifiable information unless that character of data is strictly necessary for the vendor to perform under the contract.

The Data Back End: Vendor Use of Data

The technology vendor and customer will usually promptly agree on the extent of vendor collection and uses of customer data that are strictly necessary for the vendor to provide the contracted products and services. In some cases, they may also align on select additional vendor data uses that are allowed, such as to improve the contracted products or services, to verify the customer's permitted use of the vendor's deliverables, or to conduct self-audits of its provision of the contracted offerings. In other cases, the vendor may seek less-focused data use permissions, such as for any and all business purposes (which could include, as examples, the development or distribution of artificial intelligence products or services, as well as the sale or licensing of the data to others).

In response, whether the customer is looking to restrict broad vendor rights, or the vendor is seeking to persuade the customer to permit expansive use rights, the parties

may wish to consider the following scenarios to reach agreement:

- Would it be appropriate to compensate the customer or discount the vendor's products or services in exchange for the customer permitting the vendor to use or collect customer data for more purposes than are strictly necessary to provide the contracted products or services, to use or collect more customer data than is necessary for the agreed purposes, or to gather or use customer data for longer than might otherwise be needed for the agreed purposes?
- Can the parties get comfortable with the vendor having rights to collect and use more data, to use the data for more purposes, or to collect or use the data for a longer duration, if the collection and use is limited to data that is anonymized, de-identified, pseudonymized, or aggregated?

Further considering the current dynamic nature of data availability, demand, and use rights, technology agreements involving the disclosure and use of customer data more frequently include enhanced contractual protections and mitigations than were used in the recent past. Depending on whether you are a customer or vendor, one or more the following contract terms may be invaluable to address today's heightened risks:

- For the customer, not only a vendor obligation to indemnify the customer for claims arising from impermissible use of the customer's data, but for claims related to re-identification of customer data that was previously anonymized, de-identified, pseudonymized, or aggregated. The impermissible use would include use prohibited by contract, as well as by law.
- For the customer, a grant of data use rights that is revocable in events of vendor misuse or misconduct.
- For the customer and the vendor, a warranty from the other party that it has the right to provide the data use rights granted by it under the agreement.
- For the vendor, not just a customer requirement to indemnify the vendor for claims based on the customer not having the right to disclose the data to the vendor or to permit the vendor to collect or use the data, but an indemnity and a warranty to notify the vendor of post-execution changes to the upstream rights granted to the customer by third-party data sources (which the customer, in turn, grants to the vendor).
- In the case of the vendor, an appropriately structured, qualified, and quantified limitation of liability that ties specifically and narrowly to the pertinent risks. The limitation may include a single, separate, or super dollar caps, for example, and may be limited to misuses of personal data, rather than include mishandling of corporate business data.

Bottom line, contracting for data use and collection rights will continue to get more complicated. The good news is that contractual mitigations and operational avenues to address these issues will similarly evolve. And, the size of the contract negotiated to govern particular data gathering and use rights will always be outpaced by the volume of available data worldwide.

* * * * * * * * * *

The Association of Technology Law Professionals (ATLP) welcomes all members to contribute short articles addressing legal, contractual, operational, or transactional issues of interest or concern to in-house legal counsel involved in drafting, negotiating, implementing, and managing commercial agreements involving or affecting technology. If you are interested in contributing, please contact Eric Begun at eric.begun@king-fisher.com or (214) 396-6261.

These materials are not a comprehensive review or analysis and do not include all issues that may be relevant or material to you, especially as laws change over time. Additionally, these materials are not intended as legal advice and do not create an attorney-client relationship.