Association of Technology Law Professionals

In this issue:

March 2021 Newsletter

Post-COVID Help for Corporate Legal Departments.

Updating in-house contract templates and negotiation playbooks is not sexy, nor is it directly related to a particular revenue-generating transaction. However, it may be an efficient way to address the increased pressure on in-house counsel to close more deals in less time – with fewer in-house resources and with smaller outside counsel budgets – brought on by COVID-19.

Your peers are already doing it.

Drafting and negotiating contracts is much more challenging since the outbreak of COVID-19. According to a recent Altman Weil survey, 44% of Legal departments plan to cut their 2021 budgets. HBR Consulting's 2020 Law Department Survey reveals that 84% of Legal departments are experiencing increased workloads and 18% are planning layoffs.

The Legal departments surveyed did, however, identify responsive measures. HBR Consulting reported that 70% of Legal departments have adopted templates for standard contracts and that 32% of departments plan (or have begun) to implement negotiation playbooks.

Any investment in developing, or merely updating, contract templates or negotiation playbooks is likely to pay off. The following contract issues are appearing more often and in a new light. Expedite your negotiations by proactively formalizing your attack (and fallbacks).

- ***Force Majeure.*** More frequently, force majeure clauses are no longer only two or three sentences, but are much longer. They now often additionally address notice timing, notice details, and minimum duration of non-performance for an event to qualify as force majeure.
- ***Changes in Laws.*** Changes in laws provisions are becoming more common. Customers and vendors are reacting to the prospect of unforeseen legislative and regulatory activity and are looking to avoid having no contractual mechanism to deal with events like the passage of the future version of California's consumer privacy law or the invalidation of the Privacy Shield.
- ***Business Continuity and Disaster Recovery.*** Often secondary to force majeure, now more contracts are requiring ongoing and uninterrupted performance even in disaster situations. Many agreements now tie these (new) obligations to force majeure rights.
- ***Remote workers.*** Working remotely is likely to last long beyond the pandemic. For both vendors and customers of technology, new contract terms and terminology addressing remote access and use are gaining traction as to software licensing, cloud access, and other technology user-based provisions, as well as cyber security commitments.
- ***Data Security.*** More customer template contracts are including comprehensive data security terms. Although previously common among customers in financial services, healthcare, energy, and other regulated industries, more vendors are seeing template schedules and detailed provisions from non-regulated entities.

You don't need to do a front 4½ pike into the deep end of the template and playbook pool to reap benefits. Wading into the shallow end will still generate meaningful returns.

/ by Eric Begun

Contracting Conundrum: "Reasonable Security Measures"

In technology contracts between customers and vendors, it is common to obligate one or both parties to implement "reasonable security measures" to protect applicable data and information. Typically, the obligation is a function of risk allocation or legal requirements. The recently enacted (and more recently amended) California Consumer Privacy Act's authorization of a private right of action against businesses that fail to implement reasonable security procedures and practices highlights the issue. But, what are "reasonable security measures?" And, which contracting party decides?

Often, technology contracts merely reference, but do not explain, reasonable security measures. A contract may require a party simply to "implement reasonable security measures" to safeguard applicable information. Alternatively, a contract may obligate the party to "implement reasonable security measures as required by applicable law" or to "comply with applicable data privacy and security laws, including those regarding security measures." Both customers and vendors can find these examples appealing.

Less often, but frequently when the technology transaction involves financial services companies, the contract may impose more stringent requirements based on statute or regulation. For example, the vendor may be obligated to "implement administrative, technical, and physical safeguards to insure the security and confidentiality of customer records and information, to protect against any anticipated threats or hazards to the security or integrity of such records, and to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."

Similarly, technology contracts involving healthcare information can mirror applicable federal regulations and obligate a party to "implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the information." For EU personal data, the Standard Contract Clauses (which will likely will soon change) may be invoked.

Although usually advocated by technology customers, because these more specifically stated obligations track legal requirements, they are often acceptable to the customers' vendors.

In a few cases, customers or vendors may choose to sidestep the vagueness of the above options. For example, agreements with ties to California may explicitly reference the 2016 California Data Breach Report, which specifically states that an organization's failure to implement all twenty controls in the Center for Internet Security's Critical Security Controls constitutes a lack of reasonable security. When payment card information is in scope, the contracting vendor may be directed to comply with the PCI Data Security Standards.

Increasingly more common, a technology customer – or vendor – may expressly set out detailed, bespoke security measures. The contractual statement of these measures can range from one, to three, to five or more pages.

Clearly, there are many ways for contracting parties to reach agreement on applicable security measures to be implemented under a technology contract. Be sure that what you sign up for works best for your company – all costs, risks, and consequences considered.

/ by Eric Begun

Browse-Wrap, Click-Wrap, and In-Between

For decades, online service providers and web and mobile site owners and operators have sought to bind their users to contractual terms and conditions by way of click-wrap, browse-wrap, and similar methods. For nearly as long, these parties have fought over the enforceability of such online contracting efforts. The path to an enforceable online contract should be clear by now, right?

You'd think so. Yet, even today, the formation of these agreements continues to be litigated.

The keys to binding click-wrap and browse-wrap agreements include notice, clarity, and assent. Generally speaking, a "click-wrap" agreement is one where the user must expressly manifest assent, typically by affirmatively ticking an "I agree" tick-box. A "browse-wrap" agreement, on the other hand, is one purporting to bind the user merely by being posted to the site or online service the user is accessing or using.

In Dohrmann v. Intuit (9th Cir. 2020), Intuit successfully defended the enforceability of its TurboTax click-wrap terms. The terms were conspicuously hyperlinked from the TurboTax online sign-in page, which required the user to click a sign-in button to proceed to use the service. There were three hyperlinked sets of terms, each of which appeared immediately below the sign-in button and was in a different color than the surrounding text.

In other cases decided in the past two years, some online vendors have been equally successful (see Skillz, GoSmith, and United Parcel Service), while others have not (see Huuuge and SquareTrade).

What can make an online agreement easier to enforce?

- Choose click-wrap over browse-wrap, requiring the user to affirmatively tick a box to manifest assent to the terms. Require the user to scroll through the terms or visit the pages where any hyperlinked terms appear, before the user is able to manifest assent.
- Conspicuously call out the existence and effect of the online terms. Do not require the user to scroll down the page to see the call-out. Use a font size that is no

smaller than, and has a different color than, the surrounding text.

- State the existence of any hyperlinked terms in close proximity to any "I agree" button or other tool for manifestation of user assent. Avoid hyperlinks within hyperlinked terms, and do not require the user to proceed through multiple web pages to ultimately get to the actual terms.
- Require assent to the terms when the user is first engaged by the site or online service, rather than after the user sets up an online account or receives online services. Don't just ask the user to read the terms – mandate that the user read them.
- Maintain back-office technology that reliably and accurately records each user's assent to the online terms, including the date of assent and the form of terms assented to.

/ by Eric Begun

* * * * * * * * * *

This issue's contributor:

- *Eric Begun (Partner, King & Fisher) – eric.begun@king-fisher.com*

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.

This newsletter is not a comprehensive review or analysis and does not include all issues that may be relevant or material to you, especially as laws change over time. Additionally, this newsletter is not intended as legal advice and does not create an attorney-client relationship.