Association of Technology Law Professionals

In this issue:

June 2021 Newsletter

Contractual Data Destruction Clauses are a Hot Topic

Morgan Stanley's recent payment of $60M to settle a civil proceeding for failing to properly dispose of customer data is a reminder of the importance of knowing applicable disposal laws and drafting appropriate data destruction clauses in technology agreements.

The sources of obligations to destroy or dispose of personal data are myriad. Direct and indirect federal requirements include the Gramm-Leach-Bliley ("GLB") Interagency Guidelines Establishing Information Security Standards, the GLB Safeguards Rule, the Health Insurance Portability and Accountability Act ("HIPAA") Privacy Rule, the HIPAA Security Rule, and the Fair and Accurate Credit Transactions Act Disposal Rule. Unfair and deceptive acts and practices laws, both federal and state, may also apply. In addition, at least 35 states have unique data disposal laws.

Common law negligence, invasion of privacy, and unjust enrichment are just a few other claims that may be brought against companies failing to properly destroy personal information. And, apart from these requirements, technology agreements typically include provisions requiring deletion or return of confidential information.

The data disposal requirements are not simple or easy to navigate, either. Numerous companies besides Morgan Stanley have suffered lapses, including, for example, American United Mortgage Company, Cornell Prescription Pharmacy, FileFax, CVS Pharmacy, Searchtec, Home Depot, and RadioShack.

That said, for customers contracting for technology services or products that require the use or availability of personal data, several steps are available to reduce data disposal risks.

- Know what personal information destruction and disposal laws apply. Must the destruction efforts be reasonable or must the data be rendered unreadable or undecipherable? Must the data also be unusable?
- Include agreement provisions requiring the vendor to destroy (or return) the data upon request and, in all cases, upon termination or expiration of the agreement. Add that, upon request, the vendor certify or acknowledge the destruction. Follow through on this requirement.
- Contractually require the vendor to qualitatively destroy the information so that it is permanently irretrievable, unreadable, inaccessible, and indecipherable. Mandate that paper media be shredded, disintegrated, incinerated, pulverized, or pulped.
- Contractually specify the method of data destruction, particularly if the data media may be reused. For example, obligate the vendor to wipe the data using U.S. Department of Defense (DoD) 5220.22-M standard or to clear, purge, or destroy the media according to NIST Special Publication 800-88.
- Include in the contract a right to audit the vendor's data disposal or destruction.

For technology vendors, which may also have legal obligations to destroy or dispose of data, contractual and operational mitigations also exist.

- Before contracting, know the personal information destruction and disposal laws that apply. For example, is the vendor a business associate under HIPAA?
- Proactively include language in the agreement permitting vendor destruction or disposal of the data.
- Utilize best industry practices to destroy or erase the data – even if the technology agreement does not require it.
- Segregate each customer's personal data from other customers' data, to facilitate discrete and expedient destruction or disposal.

These mitigations for technology customers and vendors are even more important, given the volume and dynamic

nature of data destruction and disposal requirements and corresponding challenges for these companies.

/ by Eric Begun

Cyber Insurance: No Lifeline for Enterprise Technology Customers

Recent major cyber attacks have kickstarted a cyber insurance buying frenzy. However, because cyber insurance coverage is unpredictable on many levels, it is critical that technology customers take meaningful steps to address insurance risks and to contract appropriately with their technology vendors.

Cyber insurance sounds great on paper but is difficult to implement effectively. Cyber insurance policies notably are not uniform or standard in providing coverage for particular occurrences, parties, or losses. Even within a particular insurance provision, contract language is unpredictable and varies widely across insurers. For example, cyber attacks initiated by state actors may or may not be covered, depending on whether the attack is considered terrorism, an act of war, or a warlike action.

Moreover, insureds and insurers routinely disagree as to the coverage and intent of cyber insurance policies. Litigation involving Mondelez, Payless Shoesource, Alorica, National Bank of Blacksburg, Sony, Target, and SS&C Technologies is just the tip of the iceberg. As for pace, let's just say that two months ago, Home Depot filed suit against three insurers to seek to obtain coverage under its policies in connection with the massive date breach it suffered *seven* years ago.

Of concern, then, enterprise technology customers frequently base their decision to accept cyber-related contractual indemnities and limitations of liability from their vendors based on the mere fact that the vendors – or the customers – have cyber liability insurance. The customers accept the risks without evaluating the vendors' purported policies and without revisiting their own coverages based on the particular technology transaction.

The following contractual and operational tips may help enterprise customers identify and mitigate cyber liability insurance related risks under their technology agreements.

- ***Read your policies.*** Technology customers should carefully review and evaluate their insurance policies, including their cyber liability policy, to determine the extent of coverage for the cyber risks for the particular technology transaction and vendor. In some cases, standard business policies (such as property insurance, crime insurance, or commercial general liability coverage) may include cyberattack losses.
- ***Summarize your policies for internal stakeholders.*** Your technology contract negotiation team will be much better able to assess applicable cyber risk for a particular technology transaction if they know the specific scope and extent of your own cyber and other insurance policies.
- ***Read your vendor's policies.*** Too often a technology customer simply includes vendor insurance requirements in its technology agreement and doesn't ask the vendor for copies of the claimed coverages. Relying on the vendor's certificate of insurance is insufficient. Ask for and read the vendor's provided policies to ensure they cover the applicable cyber risks under the agreement.
- ***Monitor policy changes.*** The technology agreement should require the vendor to provide prompt notice of changes in the vendor's insurance coverages. The agreement should establish that vendor breaches of insurance provisions specifically give rise to customer termination rights.
- ***Increase insurance coverages.*** When the customer's business team insists that the particular technology vendor is the best resource for the deal, but the vendor does not have adequate cyber insurance, the customer should consider obligating the vendor to procure sufficient coverage, even if only for the particular transaction. Be aware, however, that the vendor may seek to burden the customer with the cost of the additional coverage.

And, do keep in mind that businesses commonly underestimate the cyber coverage they need to mitigate cyber risks.

/ by Eric Begun

Is Your Technology Non-Compete Enforceable?

Frequently, software license agreements, cloud agreements, and other technology contracts include restrictive covenants or non-compete clauses that prohibit a customer from using the vendor's technology to develop competitive or substantially similar products or services. The court in Triage Logic Management and Consulting v. Innovative Triage Services examined the issue and provided a road map for saving such provisions.

In Triage Logic, the software vendor sued the customer for contracting with a third party to develop software similar to the vendor's licensed product. The vendor-customer agreement prohibited the customer from "develop[ing] similar software, services or product offerings substantially similar to the System" described in the agreement. The clause expressly survived the termination of the agreement.

The court concluded that the non-compete provision contradicted state antitrust law and, thus, was unenforceable, based on the particular restraint being indefinite and perpetual. Applicable state law barred the court from reforming the restrictive covenant to make it enforceable.

Because the Triage Logic case was decided under North Carolina law, it invites comparison to other state laws. For example, under the Texas Free Enterprise and Antitrust Act of 1983, a covenant not to compete is enforceable if it is ancillary to or part of an otherwise enforceable agreement and contains reasonable and limited parameters as to time, geography, and scope. Unlike North Carolina law, the Texas statute requires courts to reform covenants that are not reasonable and limited. A covenant not to compete is enforceable under Delaware law if it meets general contract law requirements, is reasonable in scope and duration, advances a legitimate economic interest, and balances equities. Delaware courts may, but are not required to, reform otherwise unenforceable provisions. New York law imposes a "simple rule of reason" analysis to non-compete provisions in ordinary commercial contracts (such as license agreements). New York permits blue-penciling of non-compete provisions only when the unenforceable portion of the provision is not essential, among other requirements.

When negotiating a non-compete clause in a technology agreement, technology vendors should consider the following drafting tips to increase the likelihood that the restrictive covenant is upheld.

- ***Duration.*** A perpetual or otherwise excessive duration for a non-compete provision is unlikely to be enforced, whether the duration is identified in the clause, itself, or the provision expressly survives agreement termination.
- ***Pencil Color.*** If the governing state law does not afford blue-penciling or equitable reformation, the non-compete provision may be salvageable if the contract includes a clear and permissive severability clause. Even if the governing law favors reformation, avoid a severability clause that merely instructs deletion of the offending provision.
- ***Express Rescue.*** To seek to save a non-compete clause from unenforceability, include express fallback positions in the contract to operate if primary terms (such as those regarding duration, scope, and geography) are held invalid.
- ***Purpose.*** A restrictive covenant stating a blanket prohibition, rather than one being specifically limited to competitive conduct, is less likely to be held enforceable.

On the other hand, customers seeking to defeat the application of a non-compete clause should do the opposite….

/ 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.