ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Cloud Computing Agreements: Negotiating Privacy Issues with Large Cloud Vendors

Commercial and Contracts

Technology, Privacy, and eCommerce

As in NCAA basketball, where the three-point shot has been deemed the great equalizer by which mid-major teams can slay a potential Goliath, modern-day cloud computing has played a similar role for startups. Now these small and medium-size companies can compete with large corporations in ways that they never imagined possible. The primary benefit of cloud computing is that most cloud-based contracts use a subscription model with small or no initial fees, and startups can obtain the benefits of various administrative and technology-related services without a large upfront infrastructure investment. This article is focused on reviewing privacy-related issues in vendor form agreements.

Contrary to the eight- or nine-figure deals in the Wall Street Journal, which involve armies of lawyers that spend months and hundreds of thousands of dollars in legal fees, most cloud-based subscriptions encountered by in-house attorneys are much more modest and have total transaction size in the tens of thousands. Often the vendor will have a superior bargaining position and will agree to few or no changes to a one-sided agreement. Vendors will often refuse to indemnify for privacy obligations, carve out privacy obligations from the limitations of liability section, carve out consequential damages from privacy obligations, or refuse to make any changes to their form agreement.

1. Refusal by vendor to indemnify for a breach of privacy obligations

If the vendor refuses to indemnify the cloud customer for a breach of data privacy terms, the cloud customer could seek to add a requirement that the vendor reimburse the customer for notification-related costs, such as costs relating to investigation of the breach, credit bureau monitoring services, operation of call centers, and sending notifications to affected individuals. This provision can be

defined as broadly as the vendor is willing to agree to, and may even include legal and consulting costs associated with the breach. Ideally, this reimbursement for notification-related costs would be in addition to an indemnification, but could provide an alternative if the vendor was unwilling to provide a full indemnification. In addition to an indemnification, the customer should strive for a covenant that the vendor will not breach the data privacy provisions, which may include a covenant that the vendor implement a comprehensive information security program. Likewise, if the vendor refuses to provide the indemnification, the customer could recover expectation damages for the breach of a data privacy warranty. However, one of the downsides to requesting a covenant or warranty is that the cloud customer would have to sue for breach of the agreement to recover, whereas the obligation to indemnify arises automatically under an indemnification provision.

Lastly, the cloud customer should review the termination section of the agreement and add a provision that allows the cloud customer to immediately terminate the agreement in event of the vendor's breach of its privacy obligations. The last thing a cloud customer wants is to be obligated to use a vendor who has lost the trust of its customer. Although most agreements include termination rights for an uncured material breach, it is important to clarify that a breach of privacy obligations are a material breach of the agreement.

2. Refusal by vendor to carve out a breach of privacy obligations from limitations of liability

The damages that arise from data breaches may include a variety of losses, such as notification-related costs, legal- and IT-related fees, and reputational harm. These types of damages will often exceed the damages covered in the limitations of liability provision in most vendor form agreements. According to IBM and the Ponemon Institute, in 2016 the average per-record cost of a data breach was $158. This amount was up 15 percent from the previous year and is likely to increase further.

If the vendor refuses to carve out privacy obligations from the general limitations of liability provision, then cloud customers should seek to create a separate increased cap for the vendor's breach of its privacy obligations. The privacy obligations cap can be structured in a number of ways. For instance, it could be written as a certain number, say three times, the total amount that the cloud customer pays to the vendor under the cloud agreement, or a set dollar amount. If the customer experiences vendor pushback to increase the liability cap, the cloud customer can point to the vendor's insurance coverage amount.

3. Refusal by vendor to carve out for consequential damages

In many cases, damages resulting from a breach of the vendor's privacy obligations will fall under the category of consequential or indirect damages. Accordingly, the cloud customer should seek to carve out these types of breaches from these exclusions of consequential and indirect damages. In the event that the vendor continues to resist such carve outs, the cloud customer will be provided some relief by negotiating an enhanced direct liability cap. If, however, the vendor continues to refuse to provide carve outs to the exclusions of indirect and consequential damages and the customer-negotiated reimbursement for notification-related costs, the cloud customer should attempt to expressly define that notification-related costs are direct damages, thereby allowing all such costs to be recovered under the direct damages cap.

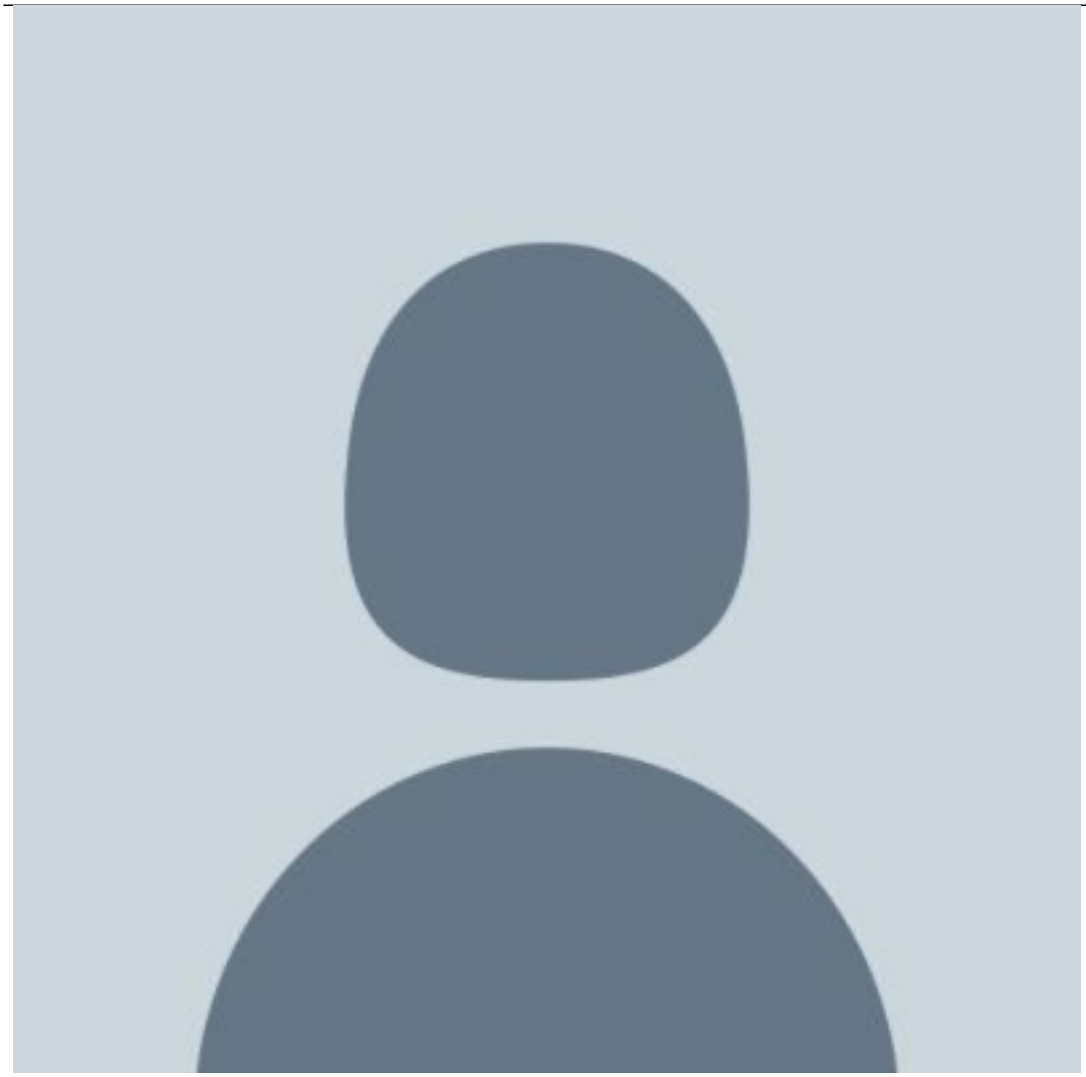
4. Refusal by vendor to agree to any changes to its standard agreement

Depending on the cloud customer's bargaining power, the vendor will often offer a "take it or leave it" contract. In these circumstances, the cloud customer should evaluate the risk and reputation of the vendor and review the type of information that will be stored on its servers. One way of evaluating the risk and reputation of the vendor is to simply ask the vendor for a copy of its corporate information security policy. The cloud customer is not creating any obligations for the vendor, but it may be a sufficient avenue to evaluate what kind of IT security the company generally maintains. If the information to be stored on the vendor's cloud-based servers is generally not considered personally identifiable information by most states (for example, email addresses, and telephone numbers), then the risks would be a lot lower than storing social security and credit card information. This analysis should be conducted with the cloud customer's business, IT, and legal teams.

Often vendors will set a per-claim or yearly cap at one or two times the fees actually paid by a cloud customer.

Please note that what is generally considered personally identifiable information (PII) in the United States is a dramatically different than what is considered PII in the European Union.

David Y. Chen

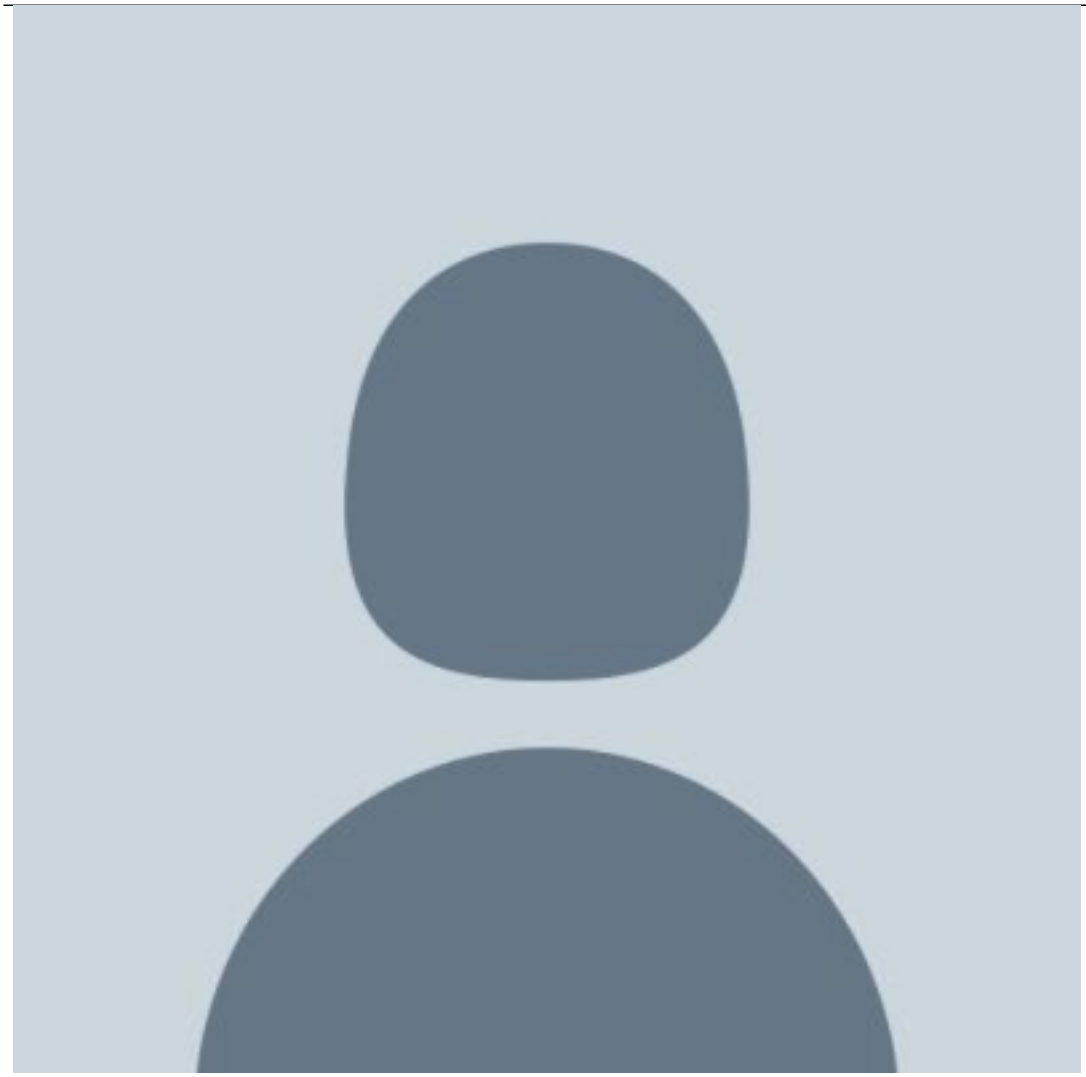


Counsel

Diamond Resorts International

David Y. Chen is counsel and legal lead for all technology and data privacy matters at Diamond Resorts International, an international hospitality company listed on the NYSE (DRII). He holds the CIPP/US, CIPP/E, CIPP/C, and CIPT certifications from the International Association of Privacy Professionals. In his spare time, he enjoys playing golf, traveling, and reading about new technological innovations.

William F. Wilson



Technology Transactions Attorney

Stoel Rives LLP

William F. Wilson is a technology transactions attorney at Stoel Rives LLP, where he helps companies manage their software and intellectual property licensing, IT, outsourcing, and data privacy needs. A certified Information Privacy Professional (CIPP/US), Wilson previously worked in the Technology Transfer office of Washington University in St. Louis. In his spare time, he likes to go backpacking in the Pacific Northwest, play the guitar, and follow the latest tech trends.