



DAILY REPORT FOR EXECUTIVES



REPORT

Reproduced with permission from Daily Report for Executives, 168 DER C-1, 9/1/2010. Copyright © 2010 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

Privacy

'Cloud' Customers Facing Contracts With Huge Liability Risks, Attorneys Say

Companies turning to third-party “cloud computing” services as a way of reducing information technology costs are typically being presented with contracts containing few, if any, terms to protect them against liability risks under data security regulations, attorneys told BNA.

Cloud service providers, such as Google Inc. and Amazon.com, are often reluctant to agree to such terms, unless forced to do so in order to win major contracts, attorneys said.

“In most situations, the contracts are not customer-friendly and there is very little ability to negotiate,” said Francoise Gilbert, managing director of IT Law Group in Palo Alto, Calif.

Generally, cloud computing allows users to store and manage data on remote computer networks operated by third parties. It can take a variety of forms, from consumers using free, advertising-supported e-mail services to companies “renting” server space and other IT capabilities over the internet at low costs.

While offering the potential for IT cost savings and other benefits, cloud computing also raises a number of privacy and security issues, attorneys said.

“Basically, you’re putting your data in someone else’s hands, without always knowing where the data will be located or what security measures will be taken,” said Gilbert, who serves as general counsel of the Cloud Security Alliance, a nonprofit organization that has developed cloud computing best practices for both customers and providers.

Significant Liability Risks Seen. The stakes are particularly high for companies that are entrusting cloud providers with sensitive, regulated information, such as health or banking records, according to Barry J. Rein-

gold, a partner in the Washington, D.C., office of Perkins Coie LLP.

“You may lose physical control over your data, but you never lose legal responsibility,” he told BNA.

Certain industries—because of the sensitive nature of the information they handle—are required by federal regulators to meet data security obligations. This includes financial institutions, under the Gramm-Leach-Bliley Act, and health care organizations, under the Health Insurance Portability and Accountability Act.

Under the Sarbanes Oxley Act, leaders of publicly traded firms are required to certify the security of internal control systems, including data protection measures.

“The CEO [chief executive officer] and other principals are liable under SOX for any misrepresentations in their financial statements,” said Luis Diaz, an intellectual property director in the Newark, N.J., office of Gibbons P.C. “There are serious penalties involved—both criminal and civil.”

The Federal Trade Commission, which oversees a wide variety of industries, has actively pursued data security cases under the “unfair or deceptive trade practices” prong of the FTC Act.

In 2006, for example, data broker ChoicePoint Inc., now a subsidiary of Reed Elsevier Inc., agreed to pay \$10 million in civil penalties and \$5 million in consumer redress to settle FTC charges that the firm’s lax data security measures resulted in a breach that compromised the personal information of more than 163,000 consumers (18 DER A-1, 1/27/06).

There are also protections for personal information under a patchwork of state data security laws.

Contracts Key. Generally, companies that outsource their IT functions to third parties, such as cloud providers, remain obligated to comply with any relevant data protection laws, according to Michael Bennett, a partner in the Chicago office of Wildman, Harrold, Allen & Dixon LLP.

In such arrangements, third-party responsibilities are mainly regulated by contract, Bennett told BNA.

“The difference between cloud computing and traditional outsourcing situations is that a cloud provider is likely to have a one-size-fits-all agreement,” he said.

Cloud providers typically offer standard, low-cost IT packages, with significant data security and privacy risks for customers and little room for contract negotiation, attorneys said.

“The providers don’t want to be in the business of insuring against problems that could happen,” said Michael Ryan, a partner at Kelley Drye & Warren LLP, Chicago. “Their business model is about having a high volume of customers. If they expand their potential liability, they risk taking a hit on their bottom line.”

Under most standard cloud agreements, the customer would have limited ability to bring claims against the provider in the event of a data security breach, Ryan said.

A standard agreement from Google, for example, includes a “limitation of liability” section that prevents the company from being held liable for any costs beyond customer fees paid over the last 12 months prior to the event giving rise to liability.

“If you have a breach, damages could potentially be much higher than that,” Ryan said.

A Google spokesman said the company takes the privacy and security of customer data “very seriously.”

“Our products are designed with security considerations upfront, not as afterthoughts, and our security team is comprised of some of the world’s leading experts in information, application and network security,” he said.

“In the unlikely event of a data breach, we would at the very least notify a customer promptly and with as much information as possible.”

When asked about the company’s willingness to negotiate over contract language, he said: “I can’t speak to negotiations of individual contracts.”

Policymakers Could Weigh In. While cloud computing is still an emerging industry, it is already gaining attention from policymakers.

The FTC, for example, has been examining the issue as part of a larger effort to develop new privacy principles in light of emerging data-collection technologies and business practices (177 DER A-8, 9/16/09).

Separately, the Electronic Privacy Information Center, a Washington-based advocacy group, has called on the commission to investigate Google’s cloud computing services (51 DER A-9, 3/19/09).

In March 2009, Google disclosed private documents saved on Google Docs Cloud Computing Service to users who lacked authorization.

Following the incident, EPIC filed a complaint with the FTC, alleging that Google had failed to implement adequate privacy and network security protections for its cloud computing services. EPIC said the Google Docs breach was just one example of many known security flaws with the company’s cloud computing services, illustrating the need for FTC intervention.

Lawmakers are also beginning to look at cloud computing. The House Oversight and Government Reform Committee, for example, is examining the benefits and challenges of a planned federal government-wide transition to the cloud (126 DER A-5, 7/2/10).

Meanwhile, at least one cloud provider has come out in support of legislation to regulate cloud computing.

Microsoft Corp., a Google competitor, unveiled a proposal in January that would, among other provisions, establish new “truth-in-cloud-computing” principles to ensure that consumers and businesses are informed about whether and how their information will be accessed and used by cloud computing service providers, as well as how it will be protected online (12 DER A-16, 1/21/10).

Under such principles, providers could be required to maintain a comprehensive information security program and to disclose a summary of it to customers, according to a white paper outlining the plan.

Providers could, for example, be required to state whether their information security programs comply with leading third-party standards, such as the International Standards Organization series (27000) for information security management, the Federal Information Security Management Act, or similar requirements, according to the proposal.

The principles could either be incorporated into a new industry self-regulatory code or federal legislation, Microsoft said.

Legal Experts Say Market Likely to Decide. Legal experts said they expect the market to address privacy and security issues surrounding the cloud over time.

“The sort of prescriptions that Microsoft is talking about are the kinds of things that companies are going to want in their contracts anyway,” Reingold said.

In response to growing concerns, some providers are already becoming more transparent about their data security practices, according to Bennett.

Increasingly, they are seeking third-party security assessments and certifications, such as the “Statement on Auditing Standards No. 70” (SAS 70), Service Organizations, an auditing statement issued by the American Institute of Certified Public Accountants Auditing Standards Board, he said.

“I think we’re at a point where cloud providers realize this is an issue,” Bennett added. “I think what they’re trying to do is develop high-level transparency that, at the same time, does not compromise security.”

Another trend is that customers are increasingly looking for more meaningful negotiations with cloud providers, according to David Navetta, a partner in the Denver office of InfoLawGroup LLP.

“Indemnification clauses, limitations on liability, consequential damage disclaimers—these are the hot issues now when it comes to cloud contracts,” Navetta told BNA. “This is really where the customer’s bargaining power comes into play. If you’re a small customer, you’re going to have less leverage. If there’s bargaining power, you often end up somewhere in the middle.”

Attorneys Urge ‘Due Diligence.’ Given the legal risks involved, attorneys said companies should take a number of steps before entering into a cloud agreement.

“The first step is to do due diligence,” Navetta said. “Consider the data involved. For certain data, it may not be a good choice to go into the cloud.”

Echoing those comments, Ryan said any company considering cloud computing should do so with “eyes wide open.”

“Do your investigation, do your due diligence, understand the data and any regulations that apply,” he said. “Weigh the risk against the reward. Make sure you’ve done your homework.”

Tanya L. Forsheit, a partner in the Los Angeles office of InfoLawGroup, told BNA that due diligence includes making an effort to find out where the provider's data centers are located, which is particularly important in assessing compliance issues under foreign privacy laws, such as the European Union's Data Protection Directive (95/46/EC).

"Some will disclose their data center locations and some won't," she said. "My speculation is that they're worried about their own liability. But, of course, in not disclosing, they are creating risks for their customers."

Another key step, according to Lothar Determann, an attorney in the Palo Alto, Calif., office of Baker & McKenzie LLP, is to seek a strong contract—ideally, one with provisions that spell out security measures the provider will take; allow the provider to be audited; detail any regulatory requirements the provider will be expected to follow; and give the customer control over its information, as much possible, including where and how it is processed.

In addition, he said customers should make sure they can be reimbursed by the provider in the event of a data security breach.

"It's important for the customer to have good indemnification requirements and to make sure the vendor is financially strong enough to make good on that," said Determann.

Along these lines, one factor that should be considered is whether the provider has cyberinsurance coverage and whether the customer can be added as part of the contract, Ryan said.

Before entering into contract negotiations, companies should make sure they are as organized as possible, Navetta said.

"These service providers handle these contracts all the time," he said. "Have a position and a fallback position. Know the terms you'd like to have in place and the ones you can live with."

Forsheit stressed that no decisions should be made without getting a consensus from all the appropriate players within the company.

"You don't want to be in a position where you have an internal conflict and you've already started talking to the provider," she said. "There may be disagreements between legal and IT or the privacy office."

Forsheit said customers should also talk to multiple providers in order to keep the process as competitive as possible.

BY ALEXEI ALEXIS

Google's standard agreement is available at http://www.google.com/apps/intl/en/terms/premier_terms.html.

Cloud Security Alliance resources are available at <http://www.cloudsecurityalliance.org/>.