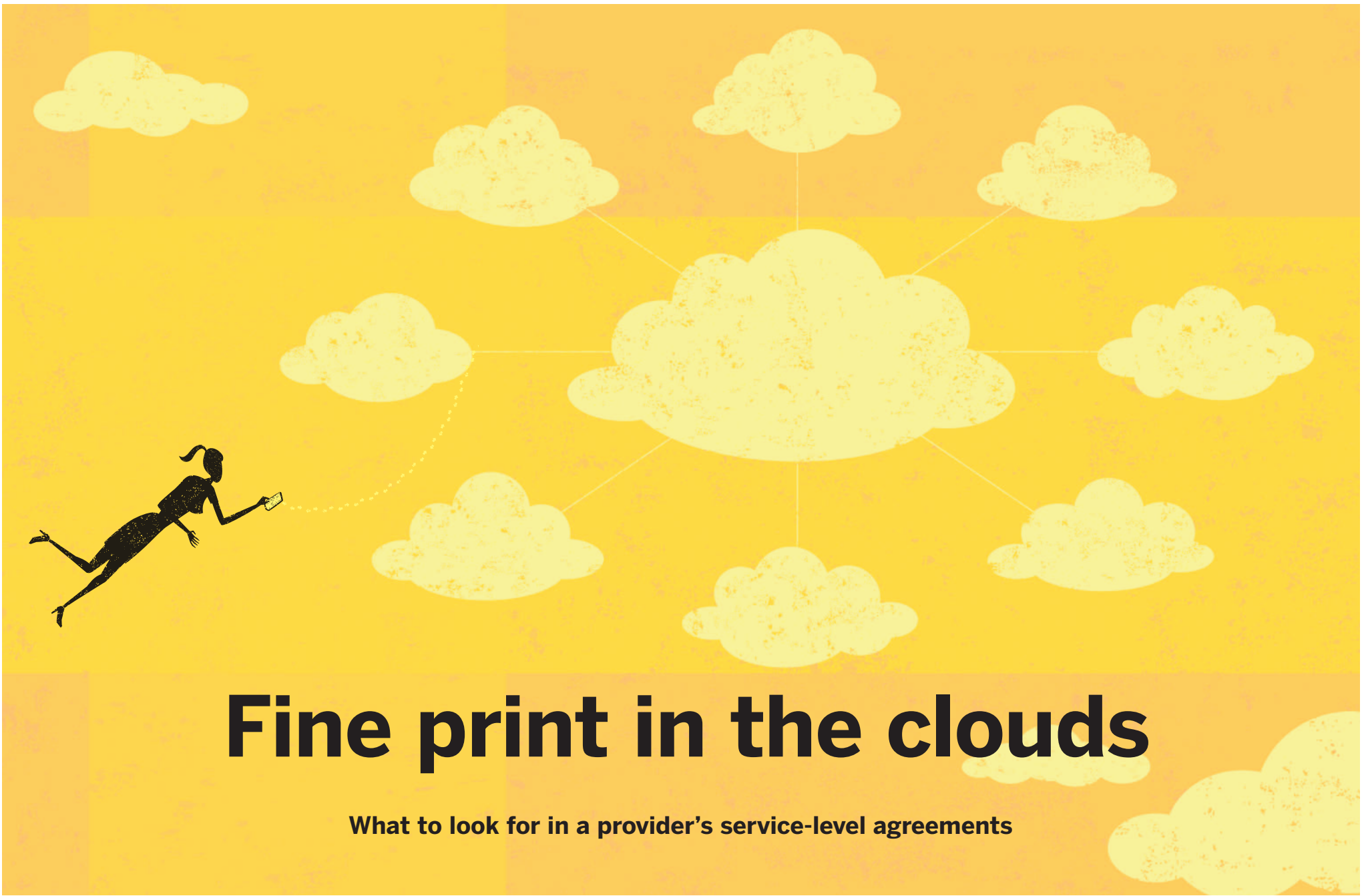
Focus

INFORMATION TECHNOLOGY



Fine print in the clouds

What to look for in a provider's service-level agreements

RETROROCKET / ISTOCKPHOTO.COM

LUIGI BENETTON

Lawyers who want to use the cloud to meet their computing needs find themselves whipsawed. Cloud service providers promise up-to-date systems, great features and manageable IT costs. But questions stemming from professional responsibilities, such as privacy and confidentiality, can curb any lawyer's enthusiasm for the cloud.

Robert Percival doesn't think this situation will last much longer. "Regulatory bodies in each Canadian province, and in other jurisdictions, like the U.K. and Scotland, are starting to realize that law firms, especially small law firms and solo practitioners, are turning to the cloud," says the Toronto-based partner and national co-chair of the technology business law group for Norton Rose Canada.

Following Percival's reasoning, legal industry regulators will create standards that cloud providers must meet for their services to be used by lawyers. In doing so, they take the guesswork out of whether a service will keep a lawyer onside with regulators. Cloud providers could evaluate their services against these standards, then market themselves to lawyers.

In the absence of such standards, lawyers can find the answers to the questions they need to ask in a cloud service provider's service-level agreements (SLAs), the commercial software version of end-user licence agreements. Here's an overview of what lawyers need to look for in cloud service provider SLAs.

Few lawyers have the time, inclination or knowledge to perform security audits of cloud providers, so they rely on warranties instead. "If a cloud provider says, 'We're providing a service and we give you no warranties whatsoever, with respect to the security we provide or against loss of data or corruption of data or disclosure of data,' that's a red flag," says Mark Hayes, managing director of Toronto-based firm Heydary Hayes PC.

Chris Bennett does not like limitation of liability. "Even if they take steps to protect your data, they'll say: 'Our maximum liability to you is three months of services.' You don't get much protection, if you get sued," says the Vancouver-based Davis LLP intellectual property lawyer.

Check where the data is stored. "Let's say your data ends up stored in a backup file somewhere in France," says Percival. "If client data is in a jurisdiction that is subject to French law, what does that do to your own professional obligations?"

Hayes advises: "If you have very sensitive information that might interest law enforcement, you will probably be very careful about storing that anywhere outside the law firm," He adds that Canadian authorities have just as much power to appropriate data as do Americans under the *U.S. Patriot Act*.

Bennett finds that privacy and confidentiality clauses are often combined. "Some service providers don't even mention privacy at all. We're always adding a privacy clause."

On-premise systems bring with them the assumption that the licensee owns the data and the software system being used, but that assumption isn't always safe in the cloud. "You want to be clear that you own your data and

Data, Page 14

Focus INFORMATION TECHNOLOGY

Without a contract, businesses at the mercy of courts

James Kosa

Handshake deals may be the stuff of Hollywood legend but in the world of information technology they can become a horror story.

A recent Ontario case involving the development of a panel for use in testing aircraft landing gear illustrates the point: *1004964 Ontario Inc. (c.o.b. t.e.s.t.) v. Aviya Technologies Inc.* [2013] O.J. No. 607.

Aviya subcontracted a portion of the work to a company that carried on business as t.e.s.t. The subcontracted work involved the development and installation of hardware and software into the test panel. Aviya would retain the development of the test cases to be run on the panel. The entire package, once completed, would be delivered by Aviya to a third party (Hispano-Suiza Canada) under an agreement between them.

Because t.e.s.t. and Aviya had had a positive and established relationship, the subcontracting proceeded with little in the way of formal documentation. Unfortunately, as the project progressed, disagreements arose as to what work was in-scope, and what was out-of-scope and, therefore, at an additional cost. The disagreements escalated, resulting in costly duplication of effort and rework by both parties, a destroyed business relationship and, ultimately, this litigation over several unpaid invoices.

An oral agreement in an IT context (as in many others) is worse than not doing the deal at all. In this case, both parties were worse off for the experience. In hindsight, it would have been cheaper for Aviya to have done the work in-house than subcontract without a contract to govern it. And t.e.s.t. would have been much better off insisting on a contract and formal specifications — even after winning in court, given the substantial costs and time invested in litigation.

Destroyed business relationship, costly litigation, expensive rework: It was a very inefficient use of business resources for both parties.

A good relationship is a reason to have a contract. If a business relationship is valuable, it is worth spending the time to clarify it when a transaction occurs. Without a written contract, businesses leave themselves at the mercy of the courts to reconstruct their dealings and decide their fate. That is what happened in this case.

The court noted that by the time they came to trial, the parties could not agree on any substantial aspect of their original business deal. "It is nearly impossible and, in my view, not necessary to repeat each of the factual disputes between the parties. They agree on very little. In fact, this case illustrates the need for a written agreement to be in place as opposed to relying upon an oral agreement based on a proposal with a third party...," Justice Thomas McEwen wrote.

The court was forced to review endless e-mail trails, invoices, and even a third-party contract to divine the intention of the parties at the time the agreement between them was formed.

In this reconstruction process, where the facts are unclear, the court was left guessing at key business terms.

One of those key terms was whether a "real-time computer" feature of the test panel was in scope or not. It was not mentioned as a requirement in any of the scant specifications or documentation, but Aviya argued that it was obviously intended to be included — "like an engine in a automobile," the automation software was a critical component.

The court found otherwise, observing that an experienced software company should not have neglected to specify something that was as important as an engine in a car if it expected it to be delivered. This is a key business lesson.

In an ideal situation, the parties would have devoted time to divide both the responsibilities and the deliverables between them in a contract. The contract would include specifications that are reasonably detailed, and where further detail may become necessary in the future, identify a process for developing and approving those additional details in a revised specification before work commences.

Changes that arise after work commences are scoped and documented separately, and treated as changes to the agreement itself, which require some level of written approval from both parties before proceeding. This whole process does not need to be onerous, and should be integrated into the regular project management and engineering functions of a technology provider when managing any project.

In an information technology agreement, specifications are the most important and typically most poorly executed part of the contract. It requires effort to get them right, but that effort is worth it to efficiently divide responsibilities.

It is not just about avoiding a dispute. Being clear about the scope of work and having a process to manage it will also guard against wasted or duplicated efforts.

In-house counsel and lawyers should urge their clients to have a contract, obviously; but, just as importantly, to treat the contracting process as a business process that can save money and mitigate real risk. The case above does not turn on abstract legal theories — it was entirely about getting the business basics right. Having a clear contract with a clear specification is not a legal exercise — it is just good business. As this case shows, courts will have little sympathy for parties that do not bother to describe the deliverables properly. What started with a handshake ended with a judgment.

James Kosa is a partner with Deeth Williams Wall in Toronto, practising in information technology and intellectual property law.

Data: Lawyers sometimes permitted to negotiate terms

Continued from page 13

that the cloud service provider cannot use your data for any other purpose than to deliver the service to you," says Jack Newton, president and CEO of Vancouver-based cloud practice management system vendor Themis Solutions Inc. "Virtually all paid services make this explicitly clear.

"If you're not paying for a product, you're the product being sold," he adds.

"Ensure the cloud provider notifies you, the account owner, if a subpoena is served on the cloud provider for your data," says Newton. "This allows you to intervene, in court if necessary, to object to that subpoena."

Data "should be encrypted, both during transmission and at end-point storage," says Martin Kratz, Calgary-based head of Bennett Jones' intellectual property practice.

Firms must also learn of any data breaches a service provider might suffer. "You need to know about it so you can carry out your responsibilities," says Kratz.

Providers need to maintain redundant systems, consisting of "hot backups," so a law practice stays operational even if the service provider's primary data centre becomes unavailable.

If a firm ends its relationship with a cloud vendor, successful transfer of firm and client data must be part of the exit scenario. The provider must delete your data when you leave the service, checking redundant servers and backups as well as main systems.

"Support during that [exit] process is very important," says Kratz. "It's a point when a cloud service provider isn't happy with a customer who's now leaving."

If a service provider's SLA doesn't meet important criteria, lawyers can try to negotiate terms in the SLA. "Some will negotiate on their agreements, others won't," says Hayes. "It depends on the particular provider and the size of your needs. How much you pay them is probably directly related to the amount of flexibility they have in their contractual relationship with you."

We want to hear from you!
Send us your verdict:
comments@lawyersweekly.ca

Lawddities

-OXFORD- / ISTOCKPHOTO.COM

Unwelcome special delivery

A Massachusetts mother is suing Federal Express on her own behalf and her two daughters, claiming it mistakenly delivered a seven-pound package of marijuana to her house, then alerted the intended recipient where to go to pick it up, Courthouse News Services reports. Maryangela Tobin filed the suit Feb. 12 in Plymouth, Mass., county court, claiming she thought the package delivered last October was a birthday present for her daughter. "Inside the package were assorted candles, candy, ribbons, markers, and crafts," the complaint said. "There were also several large vacuum-packed bags of what appeared to the Tobins to be potpourri...Maryangela broke the seal on one of the bags and the kitchen instantly filled with the odor of marijuana." Tobin's complaint states that a man came to her house 75 minutes later, asking about the package. Three "smugglers" were eventually arrested after FedEx told police it gave her address to someone else. Tobin, who claims her daughters "are now too scared to be alone in their own home for any appreciable amount of time," is seeking damages for privacy law violations, and international and reckless infliction of emotional distress and negligence. – **STAFF**