Volume 6, Issue 1, January/February 2015

SOCIALLY AWARE

THE SOCIAL MEDIA LAW UPDATE

2011 BEST LAW FIRM NEWSLETTER

IN THIS ISSUE

EDITORS

John F. Delaney
Aaron P. Rubin

CONTRIBUTORS

John F. Delaney
Adam J. Fleisher
Christopher Ford
Alistair Maughan
Julie O'Neill
Anthony M. Ramirez
Aaron P. Rubin
Scott M. Sawyer
Scott W. Stevenson

FOLLOW US

Morrison & Foerster's Socially Aware Blog

@MoFoSocMedia

MORRISON FOERSTER

Happy 2015! Welcome to the newest issue of *Socially Aware*, our Burton Award-winning guide to the law and business of social media. In this edition, we discuss key—and often ignored—legal concerns regarding social media assets in M&A transactions; we explore whether anti-Glass hysteria may have doomed Google Glass; we highlight a landmark case finding that parents can be held liable for their child's online activities (yikes!); we take a look at the FTC's latest crackdown on social media advertising; and we drill down on cloud services agreements.

All this—plus an infographic roundup of social media's "greatest" hits in 2014.

GOOD REP: SOCIAL MEDIA ASSETS IN M&A TRANSACTIONS

By Aaron P. Rubin

As we previously reported, a company's social media pages and profiles, and the associated followers, friends and other connections, may constitute valuable business assets. In our experience, however, social media assets often receive little attention in M&A transactions. Purchasers in such transactions generally require sellers to make robust representations and warranties regarding the target company's assets, but a typical purchase agreement may give social media assets only cursory treatment or, in some cases, not explicitly cover social media assets at all. In an attempt to rectify this oversight, this article outlines a set of representations and warranties that a purchaser may consider to address issues relating to a target company's social media assets in an M&A context.

To begin, it is necessary to define the category of assets at issue. In defining this category—which we will refer to as "Social Media Accounts" for convenience—a purchaser may wish to capture a broad swath of online assets not limited just to a company's pages and profiles on the major social networks (although those should certainly be addressed), including all accounts, profiles, pages, feeds, registrations and other presences on or in connection with any:

- social media or social networking website or online service;
- blog or microblog;
- mobile application;
- photo, video or other content-sharing website;
- virtual game world or virtual social world;
- rating and review website;
- wiki or similar collaborative content website; or
- message board, bulletin board or similar forum.

Armed with a broad definition of "Social Media Accounts" as described above, a comprehensive set of social media representations and warranties would require the seller to provide a list of all Social Media Accounts that the target company uses, operates or maintains, and to identify, for each such Social Media Account, any account names, user names, nicknames, display names, handles and other identifiers registered, used or held for use by or for the target company (which we will refer to collectively as "Social Media Account Names").

A typical purchase agreement may give social media assets only cursory treatment or, in some cases, not explicitly cover social media assets at all.

The purchaser may then ask the seller to make some or all of the following representations and warranties with respect to Social Media Accounts and Social Media Account Names:

- None of the Social Media Account Names infringe or otherwise violate any trademark rights or other intellectual property rights of any third party.
- All use of the Social Media Accounts complies with and has complied with (i) all terms and conditions, terms of use, terms of service and other agreements and contracts applicable to such Social Media Accounts, and (ii) applicable law and regulation.
- The target company has implemented and enforces an employee social media policy that:
  - provides that the company, and not any company employee or contractor, owns and controls the Social Media Accounts and Social Media Account Names (including all associated information and content; all relationships, interactions and communications with fans, followers, visitors, commenters, users and customers; and all associated good will and opportunities);
  - requires all employees and contractors to relinquish to the company all Social Media Account Names, passwords, and other log-in information for the Social Media Accounts upon termination of employment or engagement or at any other time upon company's request;
  - includes appropriate guidelines and restrictions regarding the use of (i) the Social Media Accounts, and (ii) personal social media accounts, including, in each case, with respect to endorsements, attribution, disclosure of proprietary information and violation of intellectual property rights; and
  - complies with applicable law and regulation.
- Each of the target company's employees and contractors has agreed in his or her company employment agreement to comply with such social media policy.
- The contemplated transaction will not result in the loss or impairment of the target company's ability to use, operate or maintain any Social Media Account or Social Media Account Name, or in the breach of any terms of use, terms of service or other agreements or contracts applicable to such Social Media Accounts.

It should be noted that a set of representations and warranties

SOCIAL MEDIA IN 2014—A LOOK BACK

Facebook[1]

- Most discussed topic (globally): World Cup
- Most discussed topic (U.S.): Ebola virus outbreak
- Most talked about athlete (U.S.): LeBron James
- Most talked about TV show (U.S.): Games of Thrones
- Most watched Ice Bucket Challenge video (U.S.): George W. Bush

Instagram[2]

- Most popular hashtag (**2nd year in a row**): #love
- Most popular photo: A wedding photo of Kim Karsdashian and Kanye West received **2.74 million likes**, making it the most-liked Instagram photo of *all time*.
- Most geotagged location: Disneyland, Anaheim, Calif.[3]

Twitter

- Most followers: Katy Perry (**61.53 million**), followed by Justin Beiber (**57.77 million**) and Barack Obama (**51.19 million**)[4]
- Most tweets/minute in **2014: 618,725** during the Germany vs. Argentina World Cup Final[5]
- Most re-tweeted: Ellen DeGeneres's Oscar selfie with Hollywood A-listers including Bradley Cooper (**3.3 million retweets**)[6]

YouTube[7]

- Most watched video: "Mutant Giant Spider Dog" (more than **128 million views**). The video features a real dog wearing a spider costume that gives him eight spider "legs"
- Second most watched video: Nike ad featuring soccer stars (more than **103 million views**)
- Third most watched video: "First Kiss" (more than **97 million views**). Pairs of strangers kiss for the first time.

NEWER SOCIAL MEDIA PLATFORMS THAT GAINED TRACTION IN 2014

SECRET: This anonymous messaging app designed for use just between friends has received $35 million in funding since it was launched in 2013.[8]

TINDER: Experts predict that this mobile dating app will have as many as 20 million active users daily by the close of 2015.[9]

MEDIUM: The White House released the State of the Union speech via this micro-blogging platform for the first time in Jan. 2015.[10]

SOURCES

1. http://newsroom.fb.com/news/2014/12/2014-year-in-review/
2. http://www.thewrap.com/instagram-shares-most-liked-pics-biggest-hashtag-of-2014-photos/
3. http://www.adweek.com/socialtimes/top-10-geotagged-locations-on-instagram-in-2014/301847
4. http://www.statista.com/statistics/273172/twitter-accounts-with-the-most-followers-worldwide/
5. http://blogs.wsj.com/digits/2014/07/14/facebook-twitter-set-usage-records-for-world-cup-final/
6. http://www.usatoday.com/story/life/2014/12/10/twitter-entertainment-highlights-most-retweeted/20142541/
7. http://www.cnn.com/2014/12/09/tech/web/top-youtube-videos-2014/
8. http://www.washingtonpost.com/blogs/the-switch/wp/2014/07/22/from-gaza-to-dating-why-users-are-confessing-their-thoughts-on-anonymous-apps-like-secret/
9. http://www.thestreet.com/story/12955209/1/unlocking-tinder-could-lead-to-5-billion-spinoff-for-iacs-dating-biz.html
10. http://www.usatoday.com/story/news/nation-now/2015/01/21/obama-sotu-twitter-facebook/22100811/

incorporating all of the points above may be more than is practical or necessary for many transactions. Purchasers will need to determine in each case how robust the social media representations and warranties should be based on the particular circumstances of the transaction, including the nature of the target company's business, the extent of the target company's use of social media and the relative negotiating positions of each party.

One last caveat: We use the term "assets" in relation to a company's social media pages and profiles advisedly, given that their legal status as property is tenuous at best (in almost all cases, these "assets" could be taken away by the third-party operators of the relevant social media platforms). But the issues addressed above are issues that we have seen arise repeatedly in reported cases, so we hope that this article will at least be helpful in thinking through some of the points that a purchaser should consider when acquiring a target company that uses social media in its business.

NARROW VISION: DID ANTI-GLASS HYSTERIA CONTRIBUTE TO THE DEMISE OF GOOGLE GLASS?

By John F. Delaney

Once the hottest new technology innovation around, Google Glass was recently put out to pasture, at least for the near future.

In the tech industry, we generally assume that a game-changing product like Glass will somehow find a way to thrive, especially with Google's virtually unlimited resources behind it. So why did Glass suffer this major setback? I don't have an answer. But I wonder if the relentless stream of negative publicity—often unreasonably negative publicity—about Glass may have contributed to consumers' reluctance to embrace the product.

> It's hard to imagine any product, no matter how innovative, surviving the barrage of negative developments related to Glass.

Consider, for example, the following items:

- A recent study allegedly showing that Glass can partially obstruct the wearer's peripheral vision received widespread coverage in the popular press. The study found that, even when the device is turned off, Glass's hardware creates a blind spot in the upper right area of the wearer's visual field. But, remarkably, this "study" *was based on the experiences of only three people*—hardly a statistically significant sample. (Most statisticians agree that, for a test to produce a meaningful result, there should be at least 100 subjects involved.)
- Another recent study picked up by the news media described the Navy's Substance Abuse and Recovery Program's treatment of a 31-year-old serviceman for alcoholism and "significant frustration and irritability related to not being able to use his Google Glass," as a case of "Google Glass addiction," as if that were an established disorder (it's not). At least the "obstructed peripheral vision" study noted above involved three participants; this "study" involved only a single subject.
- A social media consultant's claims that her Glass device was knocked off her face in a San Francisco bar received extensive national and even international press coverage, generally inciting not sympathy, but ire, for the consultant; news stories reporting her version of the events received a flood of negative comments and prompted a barrage of social media posts blaming the Glass wearer for "her failure to perceive the negative reception by bar patrons of her wearing the device and her decision to begin recording video as the situation escalated," according to one news outlet. A number of bars reportedly banned Glass in the wake of the incident.
- It was widely reported last year that Glass would make it easier for eavesdroppers to steal ATM and tablet users' PINs and passcodes—not because Glass's technology makes it superior for those purposes, but because Glass is allegedly less conspicuous than, say, a smartphone with a camera. But the fact that Glass lights up when in use would seem to make it an awkward tool for spying on people using ATMs and tablets in public.

Even a cursory Google search will turn up many other articles warning us of the perils of Glass. (We covered anti-Glass sentiment in greater detail in a blog post last year.) But I don't mean to suggest that the press was solely responsible for anti-Glass hysteria; governments and big business did their part to stoke consumer fears.

For example, several state legislatures have been considering bills that would make it illegal to wear Glass while driving. As a practical matter, for such legislation to be effective, it would have to forbid motorists from wearing any head-mounted device, whether or not it's in use—a police officer cannot be expected to know whether a person behind the wheel actually had her Glass device turned on while she was driving.

The federal government also jumped on the anti-Glass bandwagon. In May 2013, for example, a bipartisan caucus

of U.S. congressmen sent Google an inquiry regarding a variety of privacy matters. In response to that inquiry, Google announced in June 2013 that it would not allow applications with facial recognition on Glass. It's remarkable that, even in these bitterly partisan times, Glass fears could unite Democrats and Republicans.

Regulators in other countries entered the fray as well, writing to Google to complain that they had not been approached by Google to address Glass-related privacy concerns.

Further, all types of businesses and organizations have rushed to ban Glass—bars, restaurants, banks, schools, hospitals, museums, casinos, circuses, strip clubs and so on. Some of these bans, of course, make sense, but others do not; interestingly, history informs us that the revolutionary Kodak camera, upon its introduction in 1888, was banned from beach resorts and even the Washington Monument.

In any event, it's hard to imagine any product, no matter how innovative, surviving the barrage of negative developments related to Glass. Everywhere one looked, the message was that Glass had the potential to do damage—damage to its user's physical and mental health, damage to its owner's integrity, damage to the privacy of bystanders, damage to other motorists, damage to a business establishment's income.

I don't mean to suggest that Glass didn't raise some legitimate privacy concerns—it did. And so does the Internet. And social media. And mobile phones. And the Internet of Things. And even the Kodak camera, for that matter.

Now that Glass is no longer with us, perhaps we can look at it with clearer vision. Is it possible that all of the relentless criticism of Glass was, well, *short-sighted*?

FORCED TO CYBER-SPY: COURT RULES PARENTS CAN BE HELD NEGLIGENT FOR CHILD'S FACEBOOK ACTIVITY

By Scott M. Sawyer and Aaron P. Rubin

Are parents now liable for what their kids post to Facebook? According to a recent decision in the Georgia Court of Appeals, they are.

The Georgia Court of Appeals held that the parents of a seventh-grade student could be found negligent for failing to ensure that their son deleted an offensive Facebook profile that defamed a fellow classmate. The fake Facebook account depicted a fat-face caricature of the female student and featured sexual, profane and racist postings. Facebook eventually took the page down at the urging of the bullied girl's parents, more than 11 months after the school first disciplined the male student. According to the court, the failure of the boy's parents to take any action to get their son to delete the profile for nearly a year after the school alerted them about the Facebook page could constitute negligence.

"Given that the false and offensive statements remained on display, and continued to reach readers, for an additional eleven months, we conclude that a jury could find that the [parents'] negligence proximately caused some part of the injury [the girl] sustained from [the boy's] actions (and inactions)," the court stated.

The appeals court found that because the boy's parents made no attempt to view the Facebook page, learn what content their son had distributed or demand that their son delete the page, they could be held negligent for failing to police their son's social media account. For this reason, the appeals court reversed the trial court's decision to grant summary judgment to the boy's parents. The court, though, agreed with the lower court's dismissal with respect to holding the parents responsible for allowing the page to be posted in the first place.

The ruling by the Georgia Court of Appeals is currently on appeal to the Georgia Supreme Court. If upheld, this ruling could usher in a new era of parental responsibility, imposing a significant duty upon parents to monitor their children's online activity and remedy any problems once they are put on notice.

If upheld, this ruling could usher in a new era of parental responsibility, imposing a significant duty upon parents to monitor their children's online activity and remedy any problems once they are put on notice.

But will parents be upset about this holding or welcome it as they seek ways to justify their cyber-spying? More than 37% of teens own smartphones, and parents are increasingly looking for ways to keep tabs on their kids. According to the Family Online Safety Institute, 78% of parents have logged into their child's Facebook account to monitor his or her private messages. In 2012, 20 million people had already downloaded Life360, a location app that allows families to track each other's movements with by-the-minute updates. According to the co-founder of TeenSafe, an invisible tracking app that allows parents to monitor their kid's location, social media activity and text messages, more than

500,000 users have used the service to help identify online bullying and keep teens out of dangerous situations.

So the next time a teenager yells at a parent for violating his or her civil liberties by tracking all of the child's online activities, the parent can simply point to the Georgia Court of Appeals decision and say they were forced to cyber-spy, for everyone's protection.

FTC ENFORCEMENT ACTION CONFIRMS THAT AD DISCLOSURE OBLIGATIONS EXTEND TO ENDORSEMENTS MADE IN SOCIAL MEDIA

By Julie O'Neill and Adam J. Fleisher

The Federal Trade Commission (FTC) has once again made good on its promise to enforce against deceptive advertising under Section 5 of the FTC Act, *regardless of the media in which the advertising appears*: Its recently announced proposed complaint and draft settlement with the advertising firm Deutsch LA, Inc. involves endorsements posted by social media users. The action unmistakably signals to companies that advertise through social media—especially by leveraging user-generated content—that they need to comply with Section 5's disclosure requirements.

As discussed below, not only is it deceptive to post bogus endorsements, but *a clear and conspicuous disclosure of any material connection between an endorser and the advertising company is necessary in order to avoid a charge of deception*.

ONLINE ADVERTISING DISCLOSURE REQUIREMENTS UNDER SECTION 5 OF THE FTC ACT

Section 5 of the FTC Act bars "unfair or deceptive acts or practices." This prohibition extends to advertising, marketing and other promotional activities, including the use of endorsements. The FTC's Guides Concerning the Use of Endorsements and Testimonials in Advertising ("Endorsement Guides") represent the FTC's interpretation of the application of Section 5 to the use of endorsements and testimonials in advertising. *See* 16 CFR § 255. In other words, they explain how an advertiser using endorsements can avoid engaging in deceptive practices.

The action unmistakably signals to companies that advertise through social media—especially by leveraging user-generated content—that they need to comply with Section 5's disclosure requirements.

The FTC defines an "endorsement" as an advertising message that "consumers are likely to believe reflects the opinions, beliefs, findings, or experiences *of a party other than the sponsoring advertiser*." *See id.* at § 255.0(b). According to the Endorsement Guides, a customer endorsement must be from an actual, bona fide user of the endorsed product or service. In addition, if there is any material connection between the endorser and the advertiser that consumers would not reasonably expect—such as payment or other exchange of consideration, or an employment relationship—then that connection must be clearly and conspicuously disclosed. Because such information is likely to affect the weight or credibility that consumers will give to an endorsement, a failure to clearly and conspicuously disclose it is deceptive.

The FTC staff has provided guidance on how to effectively make clear and conspicuous disclosures in online advertising. When the staff initially released its Dot Com Disclosures guidance in 2000, it affirmed that Section 5 applies to online advertising, just as it applies in the brick-and-mortar world. In 2013, the FTC staff released updated Dot Com Disclosures, specifically addressing how to make appropriately clear and conspicuous disclosures online, including on mobile devices. The guidance reaffirmed that disclosures that are required to avoid deception or to otherwise comply with the law must be presented in a clear and conspicuous manner—no matter the media in which they appear—and asserted that, if an advertiser cannot make a required disclosure effectively in a particular medium, then it should not run the ad in that medium.

THE DEUTSCH LA ENDORSEMENT ACTION

The proposed settlement with Deutsch LA arose out of the advertising firm's alleged activities relating to the promotion, on behalf of its client Sony, of the PlayStation Vita handheld gaming console. (The FTC also reached a proposed settlement with Sony.) The gravamen of the FTC's complaint related to allegedly deceptive advertising claims about the console's technological capabilities. The FTC also, however, included a count relating to the advertising firm's use of Twitter to promote its client's console. Specifically, the complaint alleged that Deutsch LA employees responded to a request from an assistant account executive to use their personal Twitter accounts to post positive comments about the Sony console, using the same "#gamechanger" hashtag. The complaint includes examples of the employees' tweets,

such as "One thing can be said about PlayStation Vita… it's a #gamechanger."

The FTC alleged that the employees' tweets were deceptive because they falsely purported to be endorsements from actual users of the Sony gaming console. Moreover, the fact that the tweets were written by employees of Sony's ad agency would have been material to consumers in making decisions about whether to purchase the console. For this reason, the tweeters' failure to disclose their connection to Deutsch LA (and, in turn, to Sony) was allegedly deceptive.

In light of both the Endorsement Guides and the revised Dot Com Disclosures guidance, this FTC enforcement action is not surprising. The Endorsement Guides establish that the failure to disclose a material connection is deceptive, and Dot Com Disclosures affirm that the FTC's rules on necessary disclosures apply to any message, whatever the medium, and expressly including even "space constrained ads," such as tweets.

WHAT'S NEXT?

The *Deutsch LA* proposed consent order bars the company from representing that an endorser of a product is an independent user or ordinary consumer of the product, if that is not the case, and it requires the ad agency to make clear and prominent disclosures of any material connections between an endorser and Deutsch LA and/or entities on whose behalf it promotes a product or service. The action thus reaffirms that individual endorsements that appear in social media must clearly and conspicuously disclose any material connection between the endorser and the advertiser of the endorsed product or service.

The FTC has brought cases based on deceptive endorsements before. For instance, in 2010, *In re Reverb Communications* (also an advertising agency), the FTC alleged that Reverb's employees posted reviews in iTunes about the agency's clients' gaming applications, without disclosing their relationship to the agency or its clients. *Deutsch LA*, however, appears to be the first time that it has brought an enforcement action against endorsements made on social media. Now that the FTC has followed through on its Dot Com Disclosures guidance that tweeted ads are just like any other advertisements—and thus require the same clear and conspicuous disclosures as in any other media—the obvious question is, "what's next?" Now that social media is multimedia (See, for example, Instagram and Pinterest, which let users post photos and videos), brands are likely to leverage users to incorporate promotions into their personal feeds.

For instance, if a brand discovers that a popular Instagram user takes compelling pictures that meld with the brand's image, the brand might engage that user to produce content on behalf of the brand and to use a hashtag or some other means to promote the brand organically in the user's feed.

If the brand does not require the user to disclose—clearly and conspicuously and in each picture, tweet or other post—that he or she has a material connection to the company, then both the company and the user run the risk of being subject to a charge of deception.

SHORTER AND SIMPLER, YES—BUT IS IBM'S NEW CLOUD SERVICES AGREEMENT ANY SWEETER?

By John F. Delaney and Anthony M. Ramirez

IBM has been receiving rave reviews in the media for simplifying its Cloud Services Agreement to a mere two pages in length. And yes, the Agreement also boasts healthy margins and a normal font. But does the Agreement's reasonable length equate to reasonable terms?

After all, from a customer's perspective, shorter doesn't necessarily mean better.

Certainly IBM's new Agreement was designed to reduce negotiation. According to the International Association for Contract & Commercial Management, which declared IBM a finalist for an award because of the Agreement's simplified approach, IBM has competitively benchmarked the terms of the new Agreement and IBM apparently feels that the terms will meet the business requirements of most enterprise clients.

From a customer's perspective, shorter doesn't necessarily mean better.

Indeed, of the customers presented with IBM's new Agreement, *80 percent have reportedly signed it without negotiation*. The remaining 20 percent, however, still chose to treat the new Agreement—simplified or not—as merely IBM's opening draft.

Upon review of the new Agreement, it becomes clear why these "20 percenters" chose to negotiate.

For example, the first section of the Agreement is entitled *Service Performance and Commitments*, but the 208 words of the section contain little in the way of actual commitments. The Cloud Services are merely "designed" to be available 24/7, and while IBM agrees to provide notice of scheduled maintenance, there are no limits on the timing or duration of such maintenance.

Customers must also review the Service Description — in a separate document — to determine what, if any, license rights,

data security obligations, service levels and renewal options will apply to the Agreement.

At times, the Agreement does provide terms that a customer will want to see — such as an indemnity against third-party patent and copyright claims — but the value of these terms is often limited. (Even in the shortest contract, the devil is still in the details.)

Customers must also be careful not to skip over short statements with potentially broad implications. For example, while IBM does not ask the customer to expressly indemnify IBM, the Agreement does contain a very short — and very vague — statement making the customer "responsible for" any "violation of law or any third-party rights caused by" the customer's content uploaded to the service or other use of the service. Could this statement require that a customer indemnify IBM for claims arising from any such violation? If so, the customer's liability for such third-party claims could be unlimited, because the Agreement's limitation-of-liability provision protects only IBM, not the customer.

Service providers are often urged to keep an agreement as "short and simple" as possible, and this is unquestionably an important goal that will help to reduce costs for both parties. At the same time, anyone reviewing such an agreement should bear in mind that it may have been "shortened and simplified" by the omission of key legal protections.

Ultimately, an informed customer wants an agreement that is short, simple *and* sweet.

NEGOTIATING CLOUD CONTRACTS

By Alistair Maughan, Christopher Ford and Scott W. Stevenson

The cloud computing market is evolving rapidly. New as-a-service (aaS) platforms are appearing and the dichotomy between public and private cloud domains has been fractured into many different shades of hybrid cloud alternatives. While many of the key issues—privacy risk, data location, and service commitment—remain the same, service providers' commercial offerings are becoming more flexible.

> At this stage in cloud computing's evolution, even more so than for traditional IT contracting, the key is to know what can be negotiated and how much.

Over the past 18 months, we have even started to see changes in the "take it or leave it" approach to cloud contracts. Negotiations of cloud contracts have started to occur. But at this stage in cloud computing's evolution, even more so than for traditional IT contracting, the key is to know what can be negotiated and how much.

CLOUD MARKET

The global cloud computing market was reportedly worth approximately $157 billion in 2014, and is expected to reach $290 billion by 2018. The market is growing at an annual rate of almost 50%. North America continues to represent the largest share of the global cloud market with over 50% of the market, followed by the EMEA region with approximately 29%.

Software as a service (SaaS) is still the biggest sell, followed by infrastructure as a service (IaaS) and platform as a service (PaaS). The Big 3 aaS cloud offerings represent 90% of the global cloud market according to a recent survey.

Flexibility and cost savings are still the main drivers for customers selecting cloud services—while security and privacy remain the top concerns. Interestingly, some customers are starting to consider cloud offerings as a means of improving the security of their data, taking the view that leading cloud providers have more expertise in protecting data and are able to invest more heavily in evolving technologies.

As the cloud market continues to grow in volume terms, the diversity of the market offerings is also increasing. There is more competition than ever before in most of the main cloud market segments, with well-publicized price cuts, more service offerings and many, if not most, software providers examining ways to move into service-based offerings. Traditional market leaders, such as Microsoft and IBM, experience year-on-year growth. Reputation and cost are the key factors in cloud vendor selection, followed by performance assurance related issues.

In general, most large cloud providers are showing a renewed focus on multinational clients and also want to move up the value chain and target larger institutional clients. Outsourcing arrangements now increasingly encompass a cloud computing element, and some cloud providers are prepared to offer managed services to mimic elements of so-called "traditional" outsourcing.

Genuine adoption by regulated entities, especially financial services institutions, is the next big target; although the take-up is not helped by the reticence of regulators in some key global markets (with the notable exception of the United States) to provide a road map to assist regulated entities' engagement of the cloud model. Nevertheless, reticence to adopt a multi-tenanted cloud solution in regulated sectors is being eroded by the availability of aaS models available through virtual private cloud services and dedicated servers.

CLOUD CONTRACTS

It remains axiomatic that contracts for cloud computing services are generally implemented on the provider's terms. Even projecting forward at the current rate of evolution, it is hard to see that core principle changing. However, contract terms are increasingly negotiable to some extent; although the degree of negotiability pales in comparison with the contracting model in traditional services-based outsourcing.

In our experience there continues to be a (resigned) acceptance from most customers of the providers' terms (*i.e.*, the terms are what they are) and there's a general recognition that is the place to start. After all, if a customer organization expects customization of services and a genuine negotiation of service terms, then maybe the cloud is not the right place to be considered as a solution for those specific services.

Nevertheless, we have experienced greater negotiability compared to 18 months ago, and we anticipate that trend continuing in the future. The contracting areas where we perceive the most scope for negotiation tend to be commercially oriented issues such as price, privacy and security, scope and service levels, and liability caps. Technical areas, such as the variability of service elements that depend on specific data center features, do not lend themselves to negotiation because the shared service nature of cloud facilities limits the ability of providers to agree on changes in those areas. These are areas where customers often show their naivety of how cloud computing works by asking for changes that directly contradict the commoditized nature of the service offering. That said, some providers do not help themselves by justifying their refusal of almost every requested change based on the invariability of the technical solution, even when an issue is plainly commercial and not technical.

Among the key issues that recur in cloud contract negotiations are:

- customer control and visibility over subcontracting: there is a general reluctance of providers to allow approval of, or even to identify, subcontractors. Often, that can be for very good reasons, especially in a public cloud situation;
- the limitation of the provider's ability to change the nature of the services provided. Again, there may be very valid reasons for this depending on the nature of the services, but, typically, the negotiation ought to focus on the commercial implications of such changes rather than the basic right itself;
- privacy and data security commitments by the provider;
- rights of the provider to suspend services under circumstances such as non-payment or violation of an acceptable use policy;
- limitation of liability;
- termination assistance provisions allowing the customer to extend service for a period after termination or expiration to allow migration to the replacement solution; and
- the stretching of some common contracting provisions into some pretty unfamiliar directions. One motto to bear in mind when reviewing cloud terms is "never assume that you know what's in a provision based on its heading." Force majeure provisions are a good example. You may have thought that it would be hard to reinvent force majeure, but in some cloud instances force majeure seems to be elastic-sided enough to capture "changes in the taxation basis of services delivered via the Internet" as a force majeure event.

Another area where some providers have not helped their industry's cause is in the proliferation of complex, multi-document contract structures which are often poorly updated and oddly worded. Customers need to wade through the many pieces of paper and URL links, and with a lack of consistency among the documents frustration mounts and patience wears thin. These multi-layered contract structures are unwieldy and often, when quizzed, even the providers' representatives cannot navigate their way around them. It would be beneficial if the cloud industry generally—and some notable large cloud providers specifically—were to address this contracting approach over the next couple of years.

PRIVACY AND SECURITY

MoFo's Global Privacy + Data Security Group has already written extensively about the privacy implications of moving data to the cloud. The conjoined issues of privacy and security remain center stage in most cloud contract negotiations. The key issues generally are who is responsible for data security and how obligations should be allocated between service provider and customer. Importantly, there may be a different analysis between different types of cloud services, *e.g.*, between IaaS and SaaS, for example. But it is worth understanding the exact commercial and legal implications of a provider that commits only to be responsible for the "security of our network" and expects its customer to be responsible for the "security of its data."

Typically, of course, providers are more willing to take responsibility for the integrity of their networks, while attempting to steer clear of obligations in relation to data. However, some service providers now accept that a failure to improve their privacy offerings may compromise future growth in certain markets and be a competitive disadvantage.

So, for example, there is an increased willingness to adopt the EU model clauses for data transfer, and most of the large cloud providers are reacting to commercial pressures from Europe-

based clients to offer services from ring-fenced European data centers. Despite this, there is still a lack of appreciation among many customers for the difference between commitments in relation to data "at rest" (*i.e.*, where the data are stored) and from where data can be accessed.

PERFORMANCE

In general, most cloud contracts are still relatively light in terms of service-level commitments, with availability being the main measurement metric. There is no sign yet of widespread (or, indeed, early stage) acceptance of the EU's standardized SLA suggestions.

In terms of remedies for service failure, the concept of providing credit via further services or contract extension is still prevalent despite the illogicality (from a customer perspective) of accepting more of the same as a service remedy.

CONCLUSION

The old maxim "Be careful what you wish for" applies to the cloud market at this stage of development. Many commercial users of cloud services have chafed at the "take it or leave it" approach to cloud contracts. But, now that some degree of negotiation is becoming possible in some areas of the cloud market, it is clear that users need to understand more than ever what can realistically be negotiated.

At the same time, users need to clearly distinguish their reasons for adopting cloud solutions in the first place and understand the specific sector of the market that they are seeking to access. If users perceive the risks to be so great that contract negotiation seems essential before putting services in the cloud, it is possible that they need to consider whether the services they have in mind properly belong there in the first place.

In general, customers need to approach cloud computing transactions with realistic expectations. It is unrealistic to expect to renegotiate a provider's cloud contract terms materially on a project with a relatively low cost/value. Providers are either technically constricted or simply commercially unwilling to devote expensive commercial management time or legal resources to negotiate the terms of a project with a relatively low margin or revenue generation.