To the Cloud! Anticipating the Legal Issues in Cloud-Based Gaming

by John L. Nicholson and Jenna F. Leavitt

Given the great interest in "the cloud" from a business perspective, as well as Microsoft's popularization of the concept with its "To the Cloud!" advertising campaign, it's no wonder that many game providers are looking to the cloud as the next viable and profitable gaming platform. The cloud movement not only provides economic incentives through various subscription and pay-to-play models, but also helps defeat piracy by locking down game code and other intellectual property from potential thieves.

Cloud game providers have a lot to gain from virtualization, but moving to a cloud-based framework raises potential legal issues that should be considered.

Latency

The first big issue for gaming providers considering moving to the cloud is both a practical one and a legal one – latency. Unlike digital downloads, streaming games require both down **and** upstream communications. Further, gaming often demands instant, real-time action, so any material latency will be noticed, especially for multi-player, FPS-type or other real-time games. Currently, some game providers have tried to satisfy gamers' demand for real-time, low-latency play by operating in data centers that are physically close to the gamer. From a technical perspective, cloud gaming may present an issue because it could involve moving the game servers much farther away from the gamer, thus having the potential to lead to increased, or even significant latency. Another technical fix may be to use "tricks" similar to those used in non-cloud gaming to compensate for latency issues.

From a legal perspective, however, the move to the cloud could bring such "tricks" into the realm of patents held by the gaming company OnLive—patents which cover "twitch gameplay" over a cloud-based system. When porting a game from client-server or mobile-based platforms to a cloud-based platform, game providers should be sure to investigate whether the conversion will expose them to potential infringement liability, including the OnLive patent portfolio. This is especially important because most game providers are not the actual game developer, so game providers should also review their agreements with the game

developer to understand whether indemnification or re-development are options. Further, if the agreement is with a small game developer, the developer may not have the financial resources to indemnify the game provider, and thus the game provider should be aware of the potential risks before embarking on a cloud-based venture.

Another issue created by the latency problem is not exclusive to cloud-based gaming, but may be exacerbated by it. For example, a gamer could miss an important part of the game (such as a level requirement or a fight response) if the lag is too long and there is delay between the gamer's action and the game's response. Further, for games that require interaction for which there are prizes (e.g., tournaments) or any sweepstakes or competitions that reward the "first caller," users who did not win might claim that excess latency or lag prevented them from winning. Providers of such games should include in the rules for those events a recognition by the user that bandwidth could affect the user's ability to successfully compete and a disclaimer of responsibility from the provider for any latency-related issues.

The latency problem may be further exacerbated by the trend towards bandwidth caps both in mobile and, potentially, in residential broadband service.[1] There is a trend among telecommunications providers to limit the amount of data either provided to companies or made accessible to their users. This issue is still working its way through the legal system as well as the court of public opinion, and may eventually have an impact on all cloud-based application providers, including game companies.

Privacy and Data Security

Personal Information: As regulators around the world become more aware of privacy and data security concerns over personal information, they have become more focused on the privacy issues associated with the use of cloud-based services, including data protection. This risk was recently highlighted when Microsoft admitted to European data protection authorities that it would disclose personal information stored in its cloud service pursuant to requests from the U.S. government under the Patriot Act[2] without first notifying or seeking the permission of the user. Cloud gaming providers should provide ample disclosure on how and when a user's information will be disclosed, including in administrative or other governmental proceedings. Cloud game providers should also be aware of the various foreign privacy obligations, restrictions and requirements before moving into the cloud.

Data Breaches: Another notable issue is the centralization of data and the potential for large-scale data breaches. As more and more data from a game gets centralized in one location, such as a cloud server, that data becomes a bigger target for thieves looking to steal or release it. If the data on a local server cluster is lost, the number of customers affected and the compliance requirements for providing notice of the breach may be relatively minor. However, as Sony learned with the PlayStation Network attack, when operating on a global basis, game providers need to deal with not only the roughly 50 data breach notification laws in the U.S., but also the data breach notification regulations worldwide, such as those currently being drafted in the EU.

Litigation/E-Discovery: Use of cloud services also may create risks associated with litigation, in particular, electronic discovery ("e-discovery"). Ownership and control of the data is generally key in such cases. That is, if the game company owns the data, then it could be compelled to produce it, regardless of whether or not the game company is actually hosting the data or providing the servers. Alternatively, if ownership is unclear or unstated, then a cloud hosting company could be subpoenaed in the litigation, as a third

[1] http://hothardware.com/News/Comcast-Cuts-Customer-Off/

[2] http://www.engadget.com/2011/07/06/microsofts-patriot-act-admission-has-the-eu-up-in-arms/

party with potentially relevant information. Thus, although U.S. law would likely preclude a cloud provider from handing over a game company's data without permission pursuant to a subpoena, the same may not be true in other countries. Lawsuits (including patent suits) in foreign jurisdictions could result in a game provider's data being exposed without its authorization. Therefore, the contract with the cloud provider should be written to cover such potential situations. For additional discussion of these issues as they relate to cloud-based services in general, see this article[3] on Pillsbury's SourcingSpeak.com blog.

Intellectual Property

One unique aspect of providing gaming in the cloud is the ability to more effectively secure intellectual property. Mobile applications and web-based downloads are often easy to de-compile, reverse engineer or otherwise decipher, thus allowing for rampant piracy in the industry. Greater security not only helps game publishers, it also benefits gamers as well, as they would likely see the ability to cheat decrease substantially due to the unlikelihood of access to the game's code. Game providers should review their agreements with any hosting companies, including service levels, indemnification, and security.

Telecom

VoIP: Many games provide the ability to chat with other gamers over the Internet through the use of Voice over Internet Protocols (aka VoIP). Many countries are very sensitive about their state-operated telecom providers and could consider the games' chat services as a way for residents to get around the local telecom service. If that were to happen, the game might be regulated as a telecom provider in that country. Many cloud service providers who include VoIP functionality in their services should include in their contracts the ability to shut down chat functionality if it appears that local government regulation or oversight might occur.

Messaging and Chat Monitoring: Given the focus in the U.S. and other countries on the ability of law enforcement to monitor communications between users, gaming providers might find themselves on the receiving end of national security letters or warrants for law enforcement to monitor the communications of specific users. While generally legal with the U.S., other countries may not allow such monitoring by the U.S. or any other government. Further, if the game provider does not control the game servers, then the game provider must work with the cloud server provider to allow such monitoring and should include such provisions in its cloud agreements.

Cloud Contracts

The biggest cost advantage for companies moving to the cloud comes from moving to a multi-tenant environment. This not only allows for a shared cost environment, but also often provides for better uptime and disaster recovery. However, that savings opportunity also may come with certain risks.

Termination or Suspension of Service: Many cloud services contracts, like many software licenses, condition the game provider's ability to use the cloud service based on its compliance with an "acceptable use policy" or other terms. While seemingly appropriate for software licenses, such a provision is not likely applicable to the cloud gaming environment in which the game itself is not provided by the cloud provider. Thus, such provisions unnecessarily grant the cloud provider the ability to suspend the game provider's access if it doesn't comply. This is especially problematic for violent or sexually graphic games, which may

[3] http://www.sourcingspeak.com/2011/04/how-safe-is-your-email-in-the-cloud.html

be seen by cloud providers as violations of the acceptable use terms. Game providers should review their contracts to provide for indemnification or other protection to the cloud provider, rather than risk total game shut-off due to issues with so-called acceptable uses.

Service Levels: One of the most important parts of any cloud agreement is the service level agreement ("SLA"). The SLA typically provides information as to the proposed uptime of the cloud-based game, disaster recovery procedures, and support offerings, along with associated remedies for violations (usually credits against hosting charges or compensation based on the percentage of downtime or the severity of the problem). But, like the SLAs for typical phone service, unless you have strong bargaining chips, it's rare that cloud providers will make SLA commitments to the levels of service needed to keep gamers from complaining. Most cloud service providers offer SLAs that they are 100% certain they can meet to minimize the potential for liability. The contract then usually precludes responsibility for failures that don't fall into the defined categories. Amazon's recent EC2 outage provides a good example because the companies that didn't contract for and have in place the appropriate backup services were down for a much longer time period. This also raises the importance of backups, including who provides, secures and has access to them, as well as the frequency and level in which they are performed. Game providers should be sure to understand the backup services, if any, provided by the cloud service provider, including the speed at which the cloud provider can restore the game or user data, if and when needed.

Pricing and Other Services: Pricing of cloud services can be challenging. Most cloud providers sell their services based on the claim that companies can "dial up" or "dial down" as necessary on a utility model. Contracts should be reviewed for service modifications, such as defined increases or decreases in services throughout the term of the agreement. For example, a game provider may have only 100,000 players of its mobile app, but, once in the cloud, that number may quickly increase to millions. The game provider should attempt to account for such rapid increases in service demands by providing pre-defined needs and associated costs in the cloud contract. Similarly, a game provider should look at whether there are storage fees, whether there is access to multiple environments (e.g., development, test, and production), what kind of disaster recovery or business continuity is provided, and the ease of transitioning to another cloud provider should such a move become necessary or desired.

Conclusion

While moving to a virtualized environment may be very attractive to gaming providers from a cost and IP security perspective, it is not a move that should be taken lightly. Even if the technical problems are solved, there are a number of legal and contractual issues that game providers need to consider when thinking about moving to the cloud.

If you have any questions about the content of this advisory, please contact the Pillsbury attorney with whom you regularly work, or the authors below.

John L. Nicholson (bio)
Washington, DC
+1.202.663.8269
john.nicholson@pillsburylaw.com

Jenna F. Leavitt (bio)
Los Angeles
+1.213.488.7459
jenna.leavitt@pillsburylaw.com