MEETING OF THE MINDS

Connecting Future IP Law Leaders with the ABA Section of Intellectual Property Law

Cloud Computing: Emerging Legal Issues, Data Flows, and the Mobile User

By Daniel J. Buller and Mark H. Wittow

This article was the result of collaboration between members of the ABA's Young Lawyer Division and the Software Committee of the ABA-IPL Information Technology Division. If you are interested in this area of the law, consider becoming an active member of the Software Committee. Find out more about this and other Section committees at http://www.abanet.org/intelprop/committees.html.

The Emergence of Cloud Computing

Working with the "cloud" has become a normal part of everyday life. From legal research to word processing and file storage, computer users are able to take advantage of the cloud for a variety of tasks. Some functions may be practical and mundane, such as, for example, publishing and sharing vacation photos or chatting with friends and family. Other uses may be extremely sensitive and highly technical, such as storing and securing personal information for millions of credit card subscribers or health records for insureds. Cloud computing has become increasingly common among both businesses and individuals, and the cloud, which is essentially a metaphor for the Internet,[1] is being used in increasingly innovative ways. Generally, "cloud computing" occurs when an Internet connection delivers hardware power and software functionality to users regardless of where they are or which computers they are using. Because users merely are using the Internet to obtain their data and computing power, they are less tethered to their office, home, or even their physical computer systems, than ever before.

Traditionally, utilizing hardware and software resources required on-site computing power and disk storage space, as well as the technical human expertise necessary to implement, maintain, and secure those resources. Complicated and expensive upgrade procedures were necessary to take advantage of new developments and features available for software applications. In addition, the upgraded software (and hardware) often required upgrading licenses and increasing backup and recovery capabilities to reduce the downtime that users would experience should a software or hardware failure occur. Local administrators with specialized, technical skill-sets were historically responsible for application and hardware maintenance. In addition, the "traditional model" often involved managing a large hardware infrastructure with disparate operating systems and applications that required individual backups, monitoring, and software updates. Disaster recovery preparation entailed allocating redundant hardware, which correspondingly increased the amount of space that was physically required to support the additional equipment (the hardware "footprint"). The traditional computing model required companies (and individuals) to make a significant financial commitment to set up software and hardware resources, and these were frequently was difficult to expand when the needs of users changed.

The problems of the traditional model were mitigated to an extent by hardware innovations such as designing servers with vastly increased computing power to fit into a very small space. The consolidation of physical servers by system virtualization and centralized disk storage also helped lessen some of the expenses of the traditional model. With virtualization, one physical system provides the computing power for multiple "virtual" servers. The physical server dynamically allocates its actual resources, as the virtual servers require them. For example, the servers providing corporate e-mail and calendaring are on the same physical system ("co-tenants") as the servers that provide file and data storage. When the e-mail system has a spike in activity, the physical server is able to borrow resources from the data storage system so that end users do not experience a drag on performance. Through such innovations, the "cloud" was born.

While experts differ on a precise definition of "cloud computing,"[2] it generally involves a subscription-based service that satisfies computing and storage needs from a virtually unlimited hardware and communication infrastructure, which is managed by a third-party provider. Cloud computing allows for rapid increases in capacity or capability without the need to invest in additional infrastructure, personnel, or software licensing. As one CEO of a cloud computing provider put it, "[a] s a customer, you don't know where the resources are, and for the most part, you don't care. What's really important is the capability to access your application anywhere, move it freely and easily, and inexpensively add resources."[3]

Mobility and convenience are major factors in the rapid adoption of cloud

Daniel J. Buller is a second-year student at the Kansas University School of Law; he will graduate in May 2011. He is a member of the ABA Young Lawyers Division and numerous ABA-IPL committees, including the Software Committee. Before law school, he worked for seven years in Information Technology at High Touch, Inc., a Witchita software development company. He can be reached at dbuller@ku.edu. **Mark H. Wittow** is a partner in the Seattle office of K&L Gates. His work focuses on intellectual property and technology transactions and related litigation. He currently chairs the ABA-IPL Information Technology Division and he is a member of many ABA-IPL committees and forums. He is the former chair of the ABA-IPL Software, Online Trademarks, and Databases Committees. He can be reached at mark.wittow@klgates.com.

computing. According to the Pew Internet and American Life Project, approximately 69% of American Internet users make use of webmail services, online data storage (e.g., for pictures, videos, personal files, etc.), or software programs (e.g., word processors or spreadsheets) whose functionality is located on the Web.[4] A majority of these users say that ease and convenience of use are major reasons they use the cloud for handling these functions. Forty-one percent of cloud users say that the ability to access their data from any computer is the principal reason for their choice to use the cloud.[5]

The increasing popularity of Internet notebooks, or "netbooks," underscores the importance of mobility to the modern computer user. Netbooks are typically low-cost, lightweight laptop computers with reduced hardware capacity and processing power that are primarily designed to provide the user with access to the Internet.[6] Netbooks provide users with vast resources because the cloud is fully accessible, without requiring users to make a substantial investment in local hardware. The virtually unlimited resources available in the cloud make the local system's limited hardware capabilities irrelevant.

Cloud computing offers companies the ability to expand their resources in real time as customer demand for product increases. For example, Animoto, a software provider that converts personal photos into music videos, developed a Facebook application that took the company from 25,000 users to 250,000 users in three days. At its peak, Animoto was signing up 20,000 new users per hour. It launched the service with five virtual servers and by the end of the three days, had expanded to 3,500 servers. Animoto's ability to "scale-up" at such an incredible rate was accomplished by utilizing a cloud provider that was able to add resources as demand for product increased.[7] Mobility, ease-of-access, and the ability to inexpensively scale system resources save users time and money. But the benefits the cloud provides come at a cost. Despite the ease and flexibility that cloud computing provides to users, users should wonder precisely how their data being stored on the Web are kept and used by the cloud service providers. A great advantage to the traditional model is that the users had control over their data and could implement whatever safeguards they thought necessary to retain control. In contrast, cloud users neither possess nor control their data. Sixty-three percent of cloud users say they would be very concerned if the cloud provider kept a copy of files users wanted to delete.[8] Ninety percent of users would be very concerned if their data were to be sold to others by the cloud provider.[9]

Cloud users have no access to the physical hardware providing their storage and processor resources. The concerns under the traditional model that caused users to invest in redundant hardware and disparate backup and recovery solutions do not disappear simply by choosing to use the cloud. The users are merely trusting that the cloud service providers are taking the risks of data loss and security seriously. The users' expectations of security and reliability, and the lack of direct control the users have over the hardware providing the data and processing power, present particularly challenging problems for the cloud computing model. Users expect cloud service providers to minimize single points of failure and encrypt data. In the end, the convenience, reduced upfront costs, and impressive scalability offered by the cloud computing model will have to be balanced against the users' expectations of data control, data flow, and disaster recovery requirements.

Emerging Legal Issues

Cloud computing and storage infrastructures are vastly more powerful than ever before because governments, businesses, and individuals are developing them at an increasingly rapid pace. The uses for which these infrastructures are put in place are diverse, ranging from lucrative and mission-critical business functions to sensitive information and expressive content. Existing laws and governance models have not always been able to keep pace with these developments. As a result, the potential for legal disputes is considerable.

Privacy concerns are on the rise. In 2008, 26% of all consumer complaints received by the FTC were related to identity theft.[10] Thirty-five percent of Internet users feel their privacy has been invaded or violated in the last year due to information they provided via the Internet.[11]

With privacy concerns in mind, the Electronic Privacy Information Center (EPIC) recently filed a complaint with the Federal Trade Commission (FTC) regarding the cloud computing services offered by Google, Inc.[12] EPIC alleged that Google does not adequately safeguard the confidential information it obtains from its users and requested the FTC open an investigation into Google's Cloud Computing Services.[13] The complaint went on to suggest that the FTC enjoin Google from offering any service for which inadequate protections of privacy and security of users' data are found to exist.[14] The complaint isolated several cloud-based services offered by Google, including webmail (Gmail),[15] online document storage and editing (Google Docs),[16] integrated desktop and Internet search (Google Desktop),[17] online photo storage (Picasa Web Albums),[18] and scheduling programs (Google Calendar).[19] The customer's data residing on a Google server are critical to the architecture of each of these services.[20] According to the complaint, Google misrepresents the privacy and security of its users' data. For example, it assures users of Google Docs that their data are secure and private unless the user specifically publishes them to the Web or invites collaborators. However, Google's Terms of Service explicitly disavow any warranty or any liability for harm that might result from Google's negligence to protect the privacy and security of user data.[21]

EPIC's complaint pointed out several known flaws with Google's cloud-based services. These include disclosure of documents to users who lacked permission to view them; security flaws in Google's webmail service that exposed usernames and passwords to theft; the exposure of Google users' personal data to malicious Internet sites; and, finally, flaws that could allow malicious sites to gain full control over users' systems.[22] In addition, the complaint pointed out the inherent risks posed by users who transfer their applications and data files onto a centralized server, namely, the relinquishment of users' control over their own data.[23] The harm caused, in each of these instances, was reasonably avoidable by the adoption of "commonsense security practices, including the storage of personal data in encrypted form, rather than in clear text."[24] As a result, the complaint alleges, Google's inadequate security measures are an unfair business practice and a deceptive trade practice.[25]

User privacy rights are fundamental to EPIC's complaint. The need for clear and consistent communication of policies, practices, and capabilities is necessary for adequately meeting user expectations. Data protection practices, such as encryption—how it is used and who is employing it—are also at the heart of the complaint against Google. As the services offered by cloud providers become more sophisticated, so too should their policies and practices related to privacy and security. The privacy concerns intrinsic in the services Google offers are serious challenges to both cloud users and providers, but they can be mitigated.

Privacy concerns also have been raised in the context of the pending *Authors Guild v. Google* book search settlement, which creates a cloud-based database of searchable books.[26] In the context of the pending consideration of that settlement, groups such as the Electronic Frontier Foundation and the American Civil Liberties Union of Northern California have requested that Google keep Web search data only for a relatively short period. Google has indicated that it will not disclose personal information, but it hasn't agreed to limits on its use of the data or the time period for holding the data, and has not offered any concrete restrictions against disclosure at this stage.

From the perspective of the licensor, the terms of the software license agreement ("SLA") should fit the service being offered to limit liability. For example, it is natural for a webmail service, such as Gmail, to store the names and e-mail addresses of its users and their contacts, and there should be adequate security measures to protect this information. However, even though Google's security measures may be adequate to protect the data that users choose to store through Gmail, the licensor may not want to be responsible for storing such information. If a cloud provider does not *need* certain private information, then they could limit their liability by not gathering and storing it.

The SLAs of cloud-based applications and services generally are nonnegotiable and much more favorable to the provider than the end user. For example, Google's license agreement for its "Chrome" Web browser initially gave the company "a perpetual, irrevocable, worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute any Content which you submit, post or display on or through" the Web browser.[27] The SLA also included a clause that allowed Google to "make such Content available to other companies, organizations or individuals with whom Google has relationships for the provision of syndicated services, and to use such Content in connection with the provision of those services."[28] A debate quickly emerged among users regarding the copyright implications of the Chrome SLA. Google then acted to amend the most objectionable language.[29] As the Chrome incident illustrates, users may need to pay close attention to the language of any SLA to which they are agreeing.

Other issues in cloud computing SLAs should be examined as well. Users should be sure to have a clear understanding of how to terminate their relationship with a given cloud provider while minimizing disruption. For example, there should be a realistic migration plan in place that assures business continuity and secure access to data following the dissolution of the users' relationship with the provider.

Some user concerns regarding the portability and security of cloud-based data and communications among clouds may be addressed in industry standards organizations.[30] Among the organizations participating in that effort are the Object Management Group (OMG), the Distributed Management Task Force (DMTF), the Open Grid Forum (OGF), the Storage Networking Industry Association (SNIA), Open Cloud Consortium (OCC), the Cloud Security Alliance (CSA), and the Standards Development Organization Collaboration on Networked Resources Management (SCRM) working group. The work of those groups is at an early stage, and it is too soon to tell whether standards efforts will be successful in resolving some or all of these issues.

Cloud computing also presents some unique copyright issues. The Second Circuit Court of Appeals, in the *Cartoon Network* case, recently considered the use of cloud-based technology to deliver cable television programs.[31] TV content providers sued Cablevision, a cable TV company, which had developed a remote storage digital video recorder (RS-DVR) that allowed Cablevision's customers to preselect programs to record that would later be available for the customers to view on demand. The difference between Cablevision's RS-DVR service and traditional DVRs is that the content was stored in and transmitted over the cloud.[32]

The *Cartoon Network* case required the parties and the court to make subtle distinctions over terms that took on new meanings in light of the fact that data were being processed, stored, and transmitted from within the cloud. The court eventually decided that it did not amount to copyright infringement for Cablevision to house and maintain the hardware that enabled end users to record and watch content on demand.

The court held that the streamed buffer copies generated by Cablevision in responding to user requests, being highly transitory in nature, were not sufficiently "fixed" to qualify as copies under copyright law.

Cablevision's particular use of cloud-based technology was important for the court's decision. For example, Cablevision's RS-DVR system stored a unique copy of each program its customers chose to record and that content was available only to that individual subscriber.[33] However, the court was careful to point out that its decision does not generally permit content delivery networks to avoid all copyright liability by making copies of each item of content and associating one unique copy with each subscriber to the network, or by giving their subscribers the capacity to make their own individual copies. We do not address whether such a network operator would be able to escape any other form of copyright liability, such as liability for unauthorized reproductions or liability for contributory infringement.[34]

In conclusion, cloud computing offers rich opportunities and incredible potential that can meet the needs of users like never before; however, privacy and security concerns, legal uncertainties, and the need to understand traditional terms in new ways are emerging as considerable challenges to abandoning traditional infrastructures. The rights and legal liability for both users and cloud service providers will continue to be determined as companies and individuals use the cloud for their computing needs. Ultimately, users will choose the model that makes the most sense given their needs, which may end up being a hybrid of cloud computing and the traditional model. ■

Pros and Cons of the Cloud Computing Model

PROS	CONS
Pay-as-you-go billing model	Control and security of corporate data in the hands of a third party
Subscribe to only the services you need	No access to physical hardware
Low upfront IT costs	Limited insight and control over data redundancy and business continuity measures
Grow or "scale" your resources quickly as needed	Physical location of data unknown, giving rise to possible jurisdictional and regulatory issues
Ability to run powerful applications and access massive amounts of data on limited hardware	Service provider's contracts can be nonnegotiable and one-sided

Endnotes

[1] Cloud Computing, http:/en.wikipedia.org/w/index.php?title=Cloud_computing&oldid=293407339 (last visited May 30, 2009).

[2] J. Nicholas Hoover, *Interop: Oracle Predicts Cloud Confusion to Continue*, InformationWeek, Sept. 17, 2008, http://www.informationweek.com/news/services/hosted_apps/showArticle.jhtml?articleID=210602225.

[3] *Id.*

[4] *Cloud Computing Gains in Currency,* PewResearch.org, Sept. 12, 2008, *available at* http://pewresearch.org/pubs/948/cloud-computing-gains-in-currency.

[5] *Id.*

[6] Microsoft Encarta Online Encyclopedia, Personal Computer (2009), http://encarta.msn.com/encnet/refpages/RefArticle.aspx?refid=761557220&pn=2.

[7] Animoto's Facebook Scale-up, http://blog.rightscale.com/2008/04/23/animoto-facebook-scale-up/ (Apr. 23, 2008).

[8] *Cloud Computing Gains in Currency*, *supra* note 4.

[9] *Id.*

[10] Fed. Trade Comm'n, *FTC Releases List of Top Consumer Fraud Complaints in 2008* (Feb. 26, 2009), *available at* http://www.ftc.gov/opa/2009/02/2008cmpts.shtm (the list, contained in the publication *Consumer Sentinel Network Data Book for January–December 2008*, showed that identity theft is the number one consumer complaint).

[11] Behavioral Advertising Survey, TRUSTe (Mar. 4, 2009), *available at* http://www.truste.org/about/press_release/03_04_09.php.

[12] *See* EPIC Complaint Before the Federal Trade Commission, *In re* Google, Inc., and Cloud Computing Services (Mar. 19, 2009), *available at* http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf.

[13] *Id.*

[14] *Id.*

[15] Gmail, http://mail.google.com (last visited May 16, 2009).

[16] Google Docs, http://docs.google.com (last visited May 16, 2009).

[17] Google Desktop, http://desktop.google.com (last visited May 16, 2009).

[18] Picasa Web Albums, http://picasaweb.google.com (last visited May 16, 2009).

[19] Google Calendar, http://www.google.com/calendar (last visited May 16, 2009).

[20] EPIC Complaint, *supra* note 12.

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] *Id.*

[26] *See Google Deal with Publishers Raises Privacy Concerns*, NPR, http://www.npr.org/templates/story/story.php?storyId=111797207 (accessed Aug. 14, 2009).

[27] *Google Amends Chrome License Agreement After Objections*, PCWorld (Sept. 3, 2008), *available at* http://www.pcworld.com/businesscenter/article/150637/google_amends_chrome_license_agreement_after_objections.html.

[28] *Id.*

[29] *Id.*

[30] *See* Press Release, Cloud-Standards.org, Major Standards Development Organizations Collaborate to Further Adoption of Cloud Standards, http://cloud-standards.org/wiki/index.php?title=Press_Release (accessed Aug. 14, 2009).

[31] Cartoon Network v. CSC Holdings, Inc., 536 F.3d 121 (2d Cir. 2008), *cert. denied*, 2009 WL 1835220 (June 29, 2009).

[32] *Id.* at 124.

[33] *Id.* at 139.

[34] *Id.* at 139–40.