

THE JOHN MARSHALL REVIEW OF INTELLECTUAL PROPERTY LAW



CLOUD COMPUTING AND THE DOCTRINE OF JOINT INFRINGEMENT: 'CURRENT IMPACT' AND FUTURE POSSIBILITIES

NICOLE D. GALLI & EDWARD GECOVICH

ABSTRACT

The computing landscape is changing in that businesses – and individuals – are increasingly turning to “the cloud” for computing solutions. In an attempt to maintain patent portfolios that keep pace with the changing computing landscape, an increasing number of corporations are filing for patent protection on cloud computing related technologies. Cloud computing patents, however, may be difficult to enforce in light of current Federal Circuit case law relating to the Joint Infringement Doctrine. Two cases, *Akamai Technologies, Inc. v. Limelight Networks, Inc.* and *McKesson Technologies, Inc. v. Epic Systems Corp.*, decided by the Federal Circuit in 2010 and in 2011 respectively, were both granted an en banc rehearing to address joint infringement. Thus, the joint infringement doctrine may be poised for change. This article examines cloud computing, how the joint infringement doctrine effects cloud computing patents, and how decisions in the *Akamai* and *McKesson* cases may change the way patent practitioners go about drafting and litigating cloud computing patents.

Copyright © 2012 The John Marshall Law School



Cite as Nicole D. Galli & Edward Gecovich, Cloud Computing and the Doctrine of Joint Infringement: 'Current Impact' and Future Possibilities, 11 J. MARSHALL REV. INTELL. PROP. L. 673 (2012).

CLOUD COMPUTING AND THE DOCTRINE OF JOINT INFRINGEMENT:
'CURRENT IMPACT' AND FUTURE POSSIBILITIES

NICOLE D. GALLI & EDWARD GECOVICH

INTRODUCTION	674
I. CLOUD COMPUTING	676
A. Defined	676
B. Cloud Computing Benefits	678
C. Cloud Computing Patents	679
II. JOINT INFRINGEMENT	680
A. Definition	680
B. Current Case Law for Joint Infringement of Method Claims	681
C. Current Case Law for Joint Infringement of System Claims	683
D. Claims Directed to Cloud Computing in Light of Issues of Joint Infringement	684
E. Current Case Law May Be Poised for Change	686
1. Akamai Technologies v. Limelight Networks	686
2. McKesson Technologies v. Epic Systems	688
F. Amici Support and Opposition for Akamai and Limelight	689
G. What Will the Federal Circuit Do?	690
H. Cloud Computing Claims After Akamai and Limelight	691
III. CONCLUSION	692

CLOUD COMPUTING AND THE DOCTRINE OF JOINT INFRINGEMENT:
‘CURRENT IMPACT’ AND FUTURE POSSIBILITIES

NICOLE D. GALLI & EDWARD GECOVICH*

INTRODUCTION

In the last decade or so, the landscape for computing and how technology is delivered is rapidly changing.¹ Businesses—and individuals—are increasingly turning to “the cloud” for computing solutions.² Cloud computing is a term coined in the 1990s but used today to refer to any type of computing services provided from a remote location.³ In essence, cloud computing converts computing as product to computing as services. These services can be as limited as access to offsite hardware and storage units, typically used only by technology professionals, or more robust services that include software applications that can be used by the ordinary consumer (for example, email services like Gmail or Yahoo or Apple’s “iCloud” service), as well as everything in between.⁴ Innovation in this area is rapidly growing as technology professionals and technology services providers are focusing on new offerings and ways of providing computing options in the cloud. Microsoft, for example, spent ninety percent of its research and development budget in 2011 on cloud computing strategy and products.⁵ The federal government, often on the forefront of adopting new technological advances, is embracing the cloud as well. The Cloud First Policy published by the Federal Chief Information Officer in February of 2011 was intended to accelerate the pace at which government agencies would realize the value of cloud computing and implement such solutions.⁶

The cloud has been described as one of the most significant innovations to ever hit the technology industry.⁷ The strong push to develop and implement cloud

* © Nicole D. Galli & Edward Gecovich 2012. Nicole D. Galli is a partner in the Intellectual Property Group of Benesch Friedlander Coplan & Aronoff, resident in its Philadelphia office. She focuses her practice on complex commercial litigation, including patent and other intellectual property litigation, and intellectual property counseling. Edward Gecovich is an associate in the Intellectual Property Group of Benesch Friedlander Coplan & Aronoff, resident in its Cleveland office. He focusses his practice on patent preparation and prosecution as well as patent litigation.

¹ Todd Nielsen, *Enough Already! Cloud Computing is Here to Stay*, WIRED, (Mar. 14, 2012, 1:14 PM), <http://www.wired.com/cloudline/2012/03/cloud-here-to-stay/>.

² *Id.*

³ See John Lannon, *Today’s Business Technologies-Demystifying the Hype*, INST. OF CERTIFIED PUB. ACCOUNTANTS IN IRELAND (2011) <http://www.cpaireland.ie/UserFiles/File/students/2012%20Examinations/Exam%20Related%20Articles/F2%20IS%20Jan%202012.pdf>; Yan Han, *On the Clouds; A New Way of Computing*, 29 INFO. TECH. & LIBR. 87, 87 (2010) (discussing cloud computing services and providers as well as the costs, advantages and issues about cloud computing).

⁴ See Han, *supra* note 3, at 87 (discussing cloud computing services and providers as well as the costs, advantages and issues about cloud computing).

⁵ Nielsen, *supra* note 1.

⁶ VIVEK KUNDRU, FEDERAL CLOUD COMPUTING STRATEGY 2 (Feb. 8, 2011), *available at* <http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf>.

⁷ Todd Nielsen, *The Perfect Storm for Cloud Computing*, WIRED (Mar. 5, 2012 12:30 PM), <http://www.wired.com/cloudline/2012/03/the-perfect-storm-for-cloud-computing/>.

computing systems is further evidenced by the sharp increase in demand for technology professionals possessing cloud computing skills. The number of job postings in the cloud computing industry is growing so rapidly that there are not enough qualified workers available to meet the demand.⁸

In addition to corporations and the government embracing the cloud, individual users are also becoming more comfortable with, and willing to adapt to, the cloud. In fact, some commentators have said that the personal cloud will replace the personal computer as the center of users' digital lives by 2014.⁹ Indeed, corporations and users already have become reliant on the cloud to the point where a recent Amazon cloud outage was described as "catastrophic."¹⁰ Cloud computing is no longer mere hype and is here to stay.¹¹

In an attempt to maintain patent portfolios that keep pace with the changing computing landscape, an increasing number corporations are filing for patent protection on cloud computing related technologies.¹² Cloud computing systems typically involve multiple parties interacting with multiple components of a system in a distributed environment.¹³ As a result, drafting patent applications, and corresponding patent claims, to cover cloud computing systems and methods requires careful attention of the drafter, who must stay particularly conscious of the joint infringement doctrine, otherwise known as divided infringement. In short, joint or divided infringement is a situation where more than one actor performs all the steps or elements of a claim.¹⁴ Likewise, a patent litigator should be conscious of current joint infringement laws when formulating a strategy for litigating a cloud computing patent. Accordingly, due to the significance of this issue, this article will examine the concept of joint infringement and how it relates to cloud computing specifically.

To begin, this article will define cloud computing in general and discuss different available cloud computing structures. This article will also discuss why the computing landscape is shifting towards cloud computing and what the future trends of cloud computing look like.

This article will then define joint infringement and discuss the current case law with respect to joint infringement of both system and method claims. This article

⁸ Brandon Butler, *Talent Pool Can't Meet Skyrocketing Demand for Cloud Skills*, COMPUTERWORLD (Mar. 14, 2012), http://www.computerworld.com/s/article/9225184/Talent_pool_not_big_enough_to_meet_skyrocketing_cloud_computing_job_demand?taxonomyId=158.

⁹ *Gartner Says the Personal Cloud Will Replace the Personal Computer as the Center of Users' Digital Lives by 2014*, GARTNER (Mar. 12, 2012), <http://www.gartner.com/it/page.jsp?id=1947315>.

¹⁰ Ahmar Abbas, *Amazon Cloud Outage: The Situation is Catastrophic but Not Serious*, ITWORLD (Apr. 22, 2011), <http://www.itworld.com/cloud-computing/158617/amazon-cloud-outage-situation-catastrophic-not-serious>.

¹¹ Tom Gillis, *Criticism Abounds, but Cloud Computing Is Here to Stay*, FORBES (May 24, 2011), <http://www.forbes.com/sites/tomgillis/2011/05/24/criticism-abounds-but-cloud-computing-is-here-to-stay/>.

¹² See *Patent Application Full Text and Image Database*, U.S. PAT. & TRADEMARK OFF., <http://patft.uspto.gov/> (last visited June 5, 2012) (showing increased number of published patent applications filed in 2009 v. 2010 that contain the keywords "cloud computing").

¹³ See Diane J. Skiba, *Are You Computing in the Clouds? Understanding Cloud Computing*, 32 NURSING EDUC. PERSPECTIVES 266, 266–68. (2011).

¹⁴ Joseph T. Helmsen & Brienne S. Terril, *Claiming the Cloud: Considerations for Drafting Patent Applications Covering Cloud Computing Technologies*, BLOOMBERG LAW REPORTS 1 (Aug. 23, 2011).

will then discuss how current joint infringement case law affects drafting and litigating cloud computing patents.

Looking to the future, this article will then proceed to analyze two related cases recently argued en banc before the Federal Circuit. Specifically, this article will discuss the issues to be decided in the two cases, the arguments presented to the court, and certain arguments raised in amici briefs submitted in support of the parties in the cases. Finally, this article will also discuss how the decisions in the two recently argued cases may potentially change the way cloud computing patents are drafted and litigated in the future.

I. CLOUD COMPUTING

A. Defined

The National Institute of Standards and Technology defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources, such as networks, servers, storage, applications, and services, that can be rapidly provisioned and released with minimal management effort or service provider interaction.¹⁵ Cisco adds that a cloud is a powerful combination of cloud computing, networking, storage, management solutions, and business applications that facilitate a new generation of information technology (“IT”) and consumer services.¹⁶ Cisco also points out that these services are available on demand, and delivered economically, without compromising security or functionality.¹⁷

Thus, cloud computing is a general concept that can take on different meaning for different people. For example, an end user may access a program application, such as Gmail, provided by Google, in the cloud.¹⁸ In this example, Google’s Gmail is a cloud computing application service. Accessing the application in the cloud means that the user is not required to download or install anything on a personal computer. Rather, the user accesses Gmail over the internet. The Gmail program application, in turn, requires infrastructure such as storage space to store all emails as well as processing power to process all of the emails. Google may choose to implement its own infrastructure or Google may choose to interface its Gmail application with a second provider offering such infrastructure in the cloud. For example, a second provider may offer data storage in the cloud. In other words, the second provider

¹⁵ PETER MELL & TIMOTHY GRANCE, THE NIST DEFINITION OF CLOUD COMPUTING: RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 2 (2011), available at <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf> [hereinafter NIST DEFINITION OF CLOUD COMPUTING].

¹⁶ *Cloud*, CISCO, <http://www.cisco.com/web/solutions/trends/cloud/index.html> (last visited June 5, 2012).

¹⁷ *Id.*

¹⁸ GOOGLE, SECURITY WHITEPAPER: GOOGLE APPS MESSAGING AND COLLABORATION PRODUCTS 2 (Jan. 17, 2012), available at http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en/us/a/help/in tl/en-GB/admins/pdf/ds_gsa_apps_whitepaper_0207.pdf.

offers a cloud computing infrastructure service. If Google chooses to utilize a cloud service for its infrastructure, the result would be two cloud computing service providers acting in concert to offer a single integrated product or service to the end user.

The cloud computing model generally embodies five essential characteristics: (1) cloud computing is an on-demand self service model in which a consumer can automatically and unilaterally provision computing capabilities; (2) capabilities must be made available over a network and accessible by standard mechanisms; (3) a provider's computing resources must be pooled to serve multiple consumers using a multi-tenant model; (4) capabilities must be elastically provisioned and released to scale according to demand; and (5) cloud systems automatically control and optimize resource use.¹⁹

To provision resources means to allocate a portion of available resources to a user or to another service according to the request.²⁰ Thus, if a user requires 10MB of data storage for example, a data service provider may allocate 10MB, from a larger data store, to that particular user. While that user is using the allocated 10MB of storage, the same storage cannot be allocated to anyone else or to any other service. Once the user is finished using the storage space, however, the originally allocated 10MB may be released or de-provisioned and then re-allocated to other users or services as needed.

There are different versions of cloud computing services and different commentators break out these services in different ways. Typically, cloud computing services are broken into three categories Software-as-a-Service, Platform-as-a-Service and Infrastructure-as-a-Service.²¹ Each of these will be discussed further below. In addition, some commentators will single out cloud-based storage services, but, more commonly, such services can be seen as fitting into one of the following three categories.

The Software-as-a-Service ("SaaS") model consists of situations where the capability provided to the consumer is to use the provider's applications (i.e., software) running on a cloud infrastructure.²² As described earlier, Google's Gmail is such a service. Users of SaaS services need not be technologically inclined and frequently are ordinary consumers.²³

In contrast, a cloud computing service may also be implemented as a Platform-as-a-Service ("PaaS") model where the capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications.²⁴ Put another way, a PaaS model provides the hardware, operating system and other tools needed for a user, typically one who is at least modestly technologically proficient, to develop or implement its preferred or even proprietary software or applications. Google's application engine, for example, enables users to build a web

¹⁹ NIST DEFINITION OF CLOUD COMPUTING, *supra* note 15, at 2.

²⁰ Ye Hu et al., *Resource Provisioning for Cloud Computing*, CTR. FOR ADVANCED STUD. ON COLLABORATIVE RESEARCH 101 (2009), *available at* <http://160.80.85.34/courses/MMI/cloudResProv.pdf>.

²¹ NIST DEFINITION OF CLOUD COMPUTING, *supra* note 15, at 1–2.

²² *Id.* at 1.

²³ *Id.*

²⁴ *Id.* at 1–2.

site application.²⁵ The tools are offered via the internet so that the user does not need to download the tools to a personal computer.

Finally, a cloud computing service may be implemented as an Infrastructure-as-a-Service (“IaaS”) model where the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources.²⁶ This is the most fundamental form of cloud computing and, essentially, is the remote provision of hardware that is application neutral and can be used by technology professionals to develop the platform and applications that work best for their end users.²⁷

In addition, each of the foregoing types of cloud computing models can be deployed in different ways. For example, cloud computing models may be implemented as a private cloud in which a cloud infrastructure is provisioned for use by a single organization, a public cloud, a community cloud, or a hybrid cloud incorporating two or more cloud infrastructures.²⁸ A private cloud is typically implemented for only internal use for employees within a company or organization.²⁹ A public cloud, on the other hand, is generally available to the public, either for free or for a fee.³⁰ There are also clouds which are for a community of users, for example those with similar interests or a company and its customers.³¹

B. Cloud Computing Benefits

As previously indicated, businesses, individuals, and government are all relying on the cloud at an increasing rate.³² With the extensive benefits being realized from the cloud, its increasing popularity should not come as a surprise. At a minimum, a service provider can reduce challenges faced because the service provider does not need to worry about managing hardware and software.³³ In a broader sense, cloud computing offers the promise of agility, economics, and focus that can unlock new innovation and transform the role of IT in driving business success.³⁴ Specifically, the cloud solves fundamental IT problems by increasing IT responsiveness, reducing capital expenditures and operational overhead, providing greater flexibility and choice, and freeing up IT resources to for innovation.³⁵

²⁵ *Id.* at 2.

²⁶ *Id.*

²⁷ *Id.* at 3.

²⁸ *Id.*

²⁹ *Id.*

³⁰ *Id.*

³¹ *Id.*

³² Russell Craig et al., *White Paper—Cloud Computing in the Public Sector: Public Manager’s Guide to Evaluating and Adopting Cloud Computing*, CISCO 1 (Nov. 2009), available at http://www.cisco.com/web/about/ac79/docs/sp/Cloud_Computing.pdf.

³³ *What is Cloud Computing?*, SALESFORCE, <http://www.salesforce.com/cloudcomputing/> (last visited June 5, 2012).

³⁴ *Microsoft Private Cloud Benefits*, MICROSOFT, <http://www.microsoft.com/en-us/server-cloud/private-cloud/benefits.aspx> (last visited June 5, 2012).

³⁵ *The Benefits of Cloud Computing*, DELL, <http://content.dell.com/us/en/enterprise/cloud-computing-value-benefits> (last visited June 5, 2012).

The future for cloud computing appears positive as well. Looking ahead, the next decade of cloud computing promises new ways to collaborate everywhere.³⁶ To achieve these new ways of collaborating, organizations will be looking to combine private clouds and public clouds in IT architectures that stretch the definition of flexibility and agility.³⁷ Companies will be looking to build community focused clouds by building systems that engage their partners and “customers in cooperative processes of product and service improvement, rather than building only inward-looking systems for in-house analysis of the world outside the company’s wall.”³⁸

C. Cloud Computing Patents

Within this background of development and innovation, companies (and individuals) are seeking patent protection for cloud computing inventions. These inventions can present unique challenges to patent drafters who seek to obtain adequate coverage and protection for these inventions. Some of these challenges will be discussed herein, but first a fundamental understanding of these kinds of patents is required.

Patent claims directed to cloud computing technology can take on several forms. As discussed, cloud computing systems may be complex systems incorporating various components dispersed over a wide geographical area. For example, in a hybrid cloud computing system, a user may interact with a private cloud via the internet. The private cloud may comprise a user-facing application service, provided by a first service provider, which interacts with a data service, provided by a second service provider. That private cloud may interface with a public cloud which similarly comprises a computing service and a data service, each being provided by distinct service providers.

A hybrid cloud, as described in the example, can be framed using several different perspectives. For example, the cloud can be viewed from the perspective of a single application or data service provider.³⁹ In such an example, claims may be directed to functions being performed by, or features of, the individual service provider. Alternatively, the cloud can be viewed from a high level perspective incorporating multiple service providers.⁴⁰ In such an example, claims may be directed to functions being performed by, or features of, multiple service providers. Accordingly, patent claims directed to such a hybrid cloud may be framed using several perspectives.

In addition to the multiple ways in which a cloud computing claim may be framed, the claims may also be drafted in either method claim form or system claim form. A method claim is directed to specific steps being performed.⁴¹ In other words, a method claim recites what is being performed. A system claim, on the other hand,

³⁶ *What is Cloud Computing?*, *supra* note 33.

³⁷ John Soar, *Cloud 2.0: Are We There Yet?*, INFORMATIONWEEK (May 25, 2010 3:39 PM), <http://www.informationweek.com/blog/outourcing/229202747>.

³⁸ Jeremy Geelan, *The Future of Cloud Computing*, CLOUD COMPUTING J. (Jan. 18, 2009), <http://cloudcomputing.sys-con.com/node/771947>.

³⁹ NIST DEFINITION OF CLOUD COMPUTING, *supra* note 15, at 3.

⁴⁰ *Id.*

⁴¹ ROBERT FABER, FABER ON MECHANICS OF PATENT CLAIM DRAFTING § 4:2 (6th ed. 2011).

is directed to what is doing the performing or the components that are performing the steps of a method.⁴²

How a cloud computing claim is framed and drafted affects the claims likelihood of withstanding the pressure and scrutiny associated with litigation. The increasing complexity of a cloud computing system as the industry moves toward more hybrid and community focused clouds demands precise focus of a patent draftsman in order to draft high quality cloud computing claims that will withstand legal challenges. Patent litigators should also pay attention to increasing complexities of cloud computing systems and corresponding patent claims as the ability to enforce or invalidate such claims may change as the technology evolves and as the law changes. One issue that both patent draftsmen and patent litigators should consider is joint infringement.

II. JOINT INFRINGEMENT

A. Definition

Joint infringement is a term used to describe a situation where multiple actors, working in concert, infringe a patent claim.⁴³ Typically, a single actor, or entity, infringes a claim.⁴⁴ However, situations arise where a claim is written in such a way that it is difficult, impractical, or impossible for a single actor to infringe the claim. For example, consider an example claim reciting two steps: (1) assembling an airplane; and (2) transporting a group of passengers using the assembled airplane. In practice, the two steps would not be performed by the same actor or entity. Rather, a manufacturer would likely perform the first step while a pilot or an airline corporation that purchases the airplane from the manufacturer would likely perform the second step. Thus, in order to infringe this example claim, the two actors would need to act jointly since any one actor alone only infringes on a portion of the claim.⁴⁵

The law as to whether two actors working in concert can be found liable for jointly infringing a patent is not statutory but rather has been developed over time in the Federal Circuit. In fact, the law regarding joint infringement is still developing and may be changing, depending on the outcome of some cases currently pending in front of the Federal Circuit. As will be discussed, in addition to the existing case law regarding joint infringement of method and systems claims, two cases were recently argued before the Federal Circuit, which at the time of this writing are currently under advisement. Depending upon the positions taken by the Federal Circuit, the opinions rendered in the two cases may alter the way patent claims are drafted and litigated with respect to joint infringement.

⁴² See *Centillion Data Sys. L.L.C. v. Qwest Commc'ns Int'l, Inc.*, 631 F.3d 1279 (Fed. Cir. 2011).

⁴³ *Joint Infringement: When Multiple Actors Work in Concert*, PATENTLYO (Apr. 14, 2011), <http://www.patentlyo.com/patent/2011/04/joint-infringement-when-multiple-actors-work-in-concert.html>.

⁴⁴ *CAFC Denies Joint Infringement Claim and Maps Out Infringement Avoidance Schemes*, PATENTLYO, (Sept. 20, 2007), <http://www.patentlyo.com/patent/2007/09/cafc-denies-joi.html>.

⁴⁵ *Joint Infringement*, *supra* note 43.

B. Current Case Law for Joint Infringement of Method Claims

In *On Demand Machine Corporation v. Ingram Industries, Inc.*,⁴⁶ the doctrine of joint infringement was described by the district court in its jury instructions as follows:

It is not necessary for the acts that constitute infringement to be performed by one person or entity. When infringement results from the participation and combined action(s) of more than one person or entity, they are all joint infringers and jointly liable for patent infringement. Infringement of a patented process or method cannot be avoided by having another perform one step of the process or method. Where the infringement is the result of the participation and combined action(s) of one or more persons or entities, they are joint infringers and are jointly liable for the infringement.⁴⁷

The Federal Circuit did not analyze this instruction, except to state that “[w]e discern no flaw in this instruction as a statement of law.”⁴⁸

The jury instruction quoted in *On Demand* was later addressed in *BMC Res. Inc. v. Paymentech, L.P.*,⁴⁹ where the Federal Circuit declined to extend the doctrine of joint infringement beyond situations where one party involved in the infringement controlled or directed the other involved party’s activities or where direct infringement existed and the second party’s involvement consisted of inducing or contributing to the infringement.⁵⁰ Paymentech’s business involved processing payment transactions. The claims at issue were directed to a method for “PIN-less debit bill payment (“PDBP”) featuring the combined action of several participants, including the payee’s agent (for example, BMC), a remote payment network (for example, an ATM network), and the card-issuing financial institutions.”⁵¹ The court concluded that Paymentech did not have “direction or control” of the other parties and therefore Paymentech “did not perform or cause to be performed each and every element of the claims.”⁵²

In *BMC*, the Federal Circuit acknowledged “that the standard requiring direction or for a finding of joint infringement may in some circumstances allow parties to enter into arms-length agreements to avoid infringement.”⁵³ However, the court indicated that “this concern does not outweigh concerns over expanding the rules governing direct infringement” and instead suggested that such concerns raised by joint infringement should be “offset by proper claim drafting.”⁵⁴

The “direction or control” standard discussed in *BMC* was further clarified by the Federal Circuit in *Muniauction, Inc. v. Thomson Corp.*⁵⁵ At issue in *Muniauction*

⁴⁶ *On Demand Mach. Corp. v. Ingram Indus., Inc.*, 442 F.3d 1331 (Fed. Cir. 2006).

⁴⁷ *Id.* at 1344–45.

⁴⁸ *Id.* at 1345.

⁴⁹ *BMC Res. Inc. v. Paymentech, L.L.P.*, 498 F.3d 1373, 1379–81 (Fed. Cir. 2007).

⁵⁰ *Id.* at 1380–81.

⁵¹ *Id.* at 1376.

⁵² *Id.* at 1382.

⁵³ *Id.* at 1381.

⁵⁴ *Id.*

⁵⁵ *Muniauction, Inc. v. Thomson Corp.*, 532 F.3d 1318, 1329 (Fed. Cir. 2008).

were patent claims directed to methods for conducting “auctions of financial instruments.”⁵⁶ Claim 1 was directed to “an electronic auction system including an issuer’s computer . . . and at least one bidder’s computer . . . said bidder’s computer being located remotely from said issuer’s computer.”⁵⁷

In *Muniauction*, the Federal Circuit followed *BMC* and reiterated that “where the actions of multiple parties combine to perform every step of a claimed method, the claim is directly infringed only if one party exercises ‘direction or control’ over the entire process.”⁵⁸ The Federal Circuit went on to specify that the “direction or control” must be “such that every step is attributable to the controlling party” or the “mastermind”⁵⁹ The Federal Circuit distinguished this situation from that in which the party is merely at “arms-length cooperation” with other parties.⁶⁰

The “direction or control” standard discussed in *BMC* and in *Muniauction* was again addressed by the Federal Circuit in *Golden Hour Data Systems, Inc. v. emsCharts, Inc.*⁶¹ In *Golden Hour*, the patent at issue was directed to a “system that includes modules for dispatching emergency medical teams, tracking their movement to and from the accident scene, managing a clinical diagnosis and treatment and accurately billing the patient for the services rendered.”⁶² Claim 1 required “integrating dispatch and billing data.”⁶³ Further, the accused infringers were “two companies [that] formed a strategic partnership, enabled their two programs to work together, and collaborated to sell the two programs as a unit.”⁶⁴

Judge Newman, in her dissenting opinion in *Golden Hour* contended that, a “strategic partnership to sell the infringing system as a unit, is not immune from infringement simply because the participating entities have a separate corporate status.”⁶⁵ Nevertheless, the Federal Circuit concluded that, despite the strategic partnership formed between the parties in this case, “the evidence of direction or control was insufficient as a matter of law to uphold a finding of joint infringement.”⁶⁶

Thus, under the foregoing decisions, to be liable for joint infringement of method claims, a party must have “direction or control” over the other parties performing steps of a method claim.⁶⁷ Moreover, the party must be the “mastermind.”⁶⁸ Finally, a “strategic partnership,” in itself, is not sufficient to establish “direction or control” and “mastermind.”⁶⁹

⁵⁶ *Id.* at 1321.

⁵⁷ *Id.* at 1322.

⁵⁸ *Id.* at 1329.

⁵⁹ *Id.*

⁶⁰ *Id.*

⁶¹ *Golden Hour Data Sys., Inc. v. Emscharts, Inc.*, 614 F.3d 1367, 1380 (Fed. Cir. 2010).

⁶² *Id.* at 1369.

⁶³ *Id.* at 1369–70.

⁶⁴ *Id.* at 1371.

⁶⁵ *Id.* at 1383.

⁶⁶ *Id.* at 1380–81.

⁶⁷ *Id.* at 1380.

⁶⁸ *Id.*

⁶⁹ *Id.* at 1382–83.

C. Current Case Law for Joint Infringement of System Claims

In *NTP, Inc. v. Research in Motion, Ltd.*,⁷⁰ the issue of joint infringement was not addressed directly by the Federal Circuit, although the court did establish an important foundation for finding such infringement in system claims.⁷¹ In *NTP*, the claims were directed to sending and receiving email over a network. Part of the accused infringing system was located in Canada.⁷² At issue before the Federal Circuit was “whether the using . . . a patented invention is an infringement . . . if a component or step of the patented invention is located or performed abroad.”⁷³ The Federal Circuit concluded that “the use of a claimed system under section 271(a) is the place at which the system as a whole is put into service, i.e., the place where control of the system is exercised and beneficial use of the system obtained.”⁷⁴

Interestingly, the Federal Circuit noted that “the concept of ‘use’ of a patented method or process is fundamentally different from the use of a patented system or device.”⁷⁵ The Federal Circuit further explained:

because a process is nothing more than the sequence of actions of which it is comprised, the use of a process necessarily involves doing or performing each of the steps recited. This is unlike use of a system as a whole, in which the components are used collectively, not individually. We therefore hold that a process cannot be used ‘within’ the United States as required by section 271(a) unless each of the steps is performed within this country.⁷⁶

This distinction foreshadows the forthcoming line of cases that appear to make it easier to prove joint infringement of systems claims, in contrast to those that make it more difficult to prove joint infringement of method claims.

In *Centillion Data Sys., L.L.C. v. Qwest Commc’ns Int’l, Inc.*,⁷⁷ the Federal Circuit relied on its definition of “use” in *NTP* in order to address “the issue of infringement for ‘use’ of a system claim that includes elements in the possession of more than one actor.”⁷⁸ At issue in *Centillion* was “a system for collecting, processing, and delivering information from a service provider, such as a telephone company, to a customer.”⁷⁹ The claims were directed to a “‘back-end’ system maintained by the service provider” and a “‘front-end’ system maintained by an end user.”⁸⁰

The Federal Circuit reiterated its holding *NTP*, noting that it is not necessary for a party to “exercise physical or direct control over each individual element of the

⁷⁰ *NTP, Inc. v. Research in Motion, Ltd.*, 418 F.3d 1282 (Fed. Cir. 2005).

⁷¹ *Id.* at 1317.

⁷² *Id.* at 1290.

⁷³ *Id.* at 1315.

⁷⁴ *Id.* at 1317.

⁷⁵ *Id.*

⁷⁶ *Id.* at 1318.

⁷⁷ *Centillion Data Sys., L.L.C. v. Qwest Commc’ns Int’l, Inc.*, 631 F.3d 1279 (Fed. Cir. 2011).

⁷⁸ *Id.* at 1283–84.

⁷⁹ *Id.* at 1281.

⁸⁰ *Id.*

system” in order to “use” the system.⁸¹ In other words, a party may infringe a claimed system by using *the system*, even if the party is not in direct physical control or possession of *each element* the system.⁸² Similarly, “supplying the software for the customer to use is not the same as using the system.”⁸³ Thus, even though a party “may make the back-end processing elements” of a system, the party may not infringe a claimed system because the party “never ‘uses’ the entire claimed system because it never puts into service the personal computer data processing means.”⁸⁴

Thus, to summarize, in order to determine whether a system that includes elements in the possession of more than one actor is infringed, it is important to consider whether any single actor has used all of the elements of the claimed system.

D. Claims Directed to Cloud Computing in Light of Issues of Joint Infringement

As discussed, the increasing complexity of cloud computing systems coupled with the fact that claims directed to cloud computing systems can be framed and drafted in various forms can lead to potential joint infringement issues. Accordingly, patent practitioners should pay close attention to existing case law and develop strategies accordingly.

A draftsman preparing a patent application for cloud computing technology should begin by working closely with the inventor of the technology to thoroughly understand the different components of the system and how they interact with each other. It is also important for the draftsman to understand who owns, maintains, and licenses the different components. Not all cloud systems have the same architecture so working with the inventor to understand the architecture of the specific system of interest will help prepare the draftsman to draft a high quality patent application.

As discussed thus far, it is difficult to successfully argue joint infringement under current case law. Thus, the best strategy is to avoid the need to argue such positions by planning ahead and preparing patent claims that are written from the perspective of a single entity. This is not always straightforward for a cloud computing system however. Because cloud systems are scalable and extensible, individual functions or components can easily be plugged in or removed from the system.⁸⁵ Therefore, even though a certain component may originally be designed and implemented by a first service provider, that same component may later be outsourced to a second service provider. Thus, an element of a cloud computing claim that was originally under a first entity’s control may later be controlled by a second entity. In addition to having a good understanding of the cloud system and how the components interact, drafting claims creatively to cover multiple embodiments, broad as well as narrow, should help offset the uncertainty of how the components of a cloud system could end up being implemented and controlled in the future.

⁸¹ *Id.* at 1284.

⁸² *Id.*

⁸³ *Id.* at 1286.

⁸⁴ *Id.*

⁸⁵ Robin Hastings, *Cloud Computing*, COLLABORATION 2.0, at 10, 11 (May/June 2009).

It is also important to consider who the accused infringer will be when the claims are ultimately enforced. Traditionally, drafting claims from a user's perspective has not been an important strategy since the user is typically not a good target (from a monetary perspective) for enforcing a patent claim. With cloud computing however, that is no longer the case. Corporations of all sizes are now the users of various types of cloud systems. Salesforce.com, for example provides cloud applications used extensively by large corporations such as NBC Universal and GE Capital.⁸⁶ Entities like these could be likely targets for enforcing patent claims, even though they are the users.

Thus, because there could potentially be more than one target for enforcing a patent claim against, it may be a good idea to draft multiple sets of claims directed to different parties. For example, a patent draftsman could prepare a first patent application and a corresponding set of claims directed at the user of a cloud system and also prepare a second patent application and a corresponding set of claims directed at the provider of a cloud system. Finally, in deciding which types of potential infringers to target, a patent draftsman should keep in mind which entities or actors are most likely to be detected of infringing a claim. It may be obvious when a service provider is offering a system that infringes a claim but it may be more difficult to determine who the users of that cloud system are.⁸⁷

Finally, because the Federal Circuit has taken a different approach to the joint infringement doctrine as applied to system claims versus method claims, drafting both types of claims may help ensure better protection for the patent owner.

From a litigation perspective, plaintiffs need to be aware of the potential challenges to be faced when arguing joint infringement of claims given the current Federal Circuit precedent making such claims difficult to win.⁸⁸ If the plaintiff has no other option other than to assert a joint infringement claim, the plaintiff should focus on the relationships with the different parties involved. When a cloud system incorporates multiple services offered by multiple providers, there is likely some form of contract that governs the relationships.⁸⁹ A plaintiff thus should look to those contracts to try and establish the necessary "direction or control" and "mastermind" of a single entity.⁹⁰ For a system claim, the plaintiff should look to the user of the cloud system as well as the service provider to determine if anyone "used" all of the components of the system.⁹¹

On the flip side, defendants in a litigation should also focus on their relationships with other service providers and try and show lack of "direction or control" over the allegedly infringing activities.⁹² Indeed, companies who are aware

⁸⁶ *Social Enterprise Stories*, SALESFORCE, <http://www.salesforce.com/customers/> (last visited June 5, 2012).

⁸⁷ See Jennifer Webb, *Stormy Weather Ahead: Enforcing Patent Rights in the "Cloud,"* IP OSGOODE (Dec. 2, 2011), <http://www.iposgoode.ca/2011/12/stormyweatheraheadenforcingpatentrightsinthecloud>; Helmsen & Terril, *supra* note 14, at 3.

⁸⁸ *Muniauction, Inc. v. Thomson Corp.*, 532 F.3d 1318, 1328 (Fed. Cir. 2008).

⁸⁹ *Int'l Bus. Mach. Corp. v. Visentin*, No. 11-CIV-399, 2011 WL 672025, at *1 (S.D.N.Y. Feb. 16, 2011).

⁹⁰ *BMC Res., Inc. v. Paymentech, L.P.*, 498 F.3d 1373, 1381 (Fed. Cir. 2007); *Muniauction*, 532 F.3d at 1329.

⁹¹ *Muniauction*, 532 F.3d at 1329.

⁹² *BMC*, 498 F.3d at 1380.

that they may face potential challenges to their activities should take this into account when drafting contracts that would cover these activities. In addition, unless the Federal Circuit decides to change the current joint infringement doctrine, potential defendants may elect to implement strategies such as looking to partner with other service providers, rather than providing an entire patented cloud system individually, in order to avoid infringing patented cloud systems.⁹³

E. Current Case Law May Be Poised for Change

Two cases, *Akamai Technologies, Inc. v. Limelight Networks, Inc.*⁹⁴ and *McKesson Technologies, Inc. v. Epic Systems Corp.*,⁹⁵ decided by the Federal Circuit in 2010 and in 2011 respectively, were both granted an en banc rehearing to address joint infringement specifically. Although it is difficult to predict, this may be an indication that the Federal Circuit is ready to adopt some changes to the joint infringement doctrine. Notably, the recently legislated America Invents Act, the most significant change to the United States patent system in a long time, did not address joint infringement.⁹⁶ The difficulties experienced by patent holders who seek to enforce method claims in the face of joint infringement claims, at least for method claims, may further provide an impetus to the Federal Circuit for making a change to the doctrine.

At the time of this writing, the oral arguments in the appeals of both *Akamai* and *McKesson* have been completed, but opinions have not yet been rendered by the Federal Circuit.⁹⁷

1. Akamai Technologies v. Limelight Networks

At issue in *Akamai* were three patents obtained by Akamai, all of which “disclose a system for allowing a content provider to outsource the storage and delivery of discrete portions of its website content.”⁹⁸ The system disclosed in Akamai’s patents were intended to address known content delivery problems on the web by providing “a scalable solution to that could efficiently deliver large amounts of web content and handle flash crowds.”⁹⁹

A typical web site includes a base document and one or more URL links to embedded objects.¹⁰⁰ The claims of the patents are directed to a “content delivery

⁹³ *Id.* at 1381.

⁹⁴ *Akamai Tech., Inc. v. Limelight Networks, Inc.*, 629 F.3d 1311 (Fed. Cir. 2010).

⁹⁵ *McKesson Tech., Inc. v. Epic Sys. Corp.*, No. 2010-1291, 2011 WL 2173401 (Fed. Cir. Apr. 12, 2012).

⁹⁶ See Pub. L. No. 112–29, 125 Stat. 284 (2011).

⁹⁷ See *Federal Circuit Hears Oral Argument on Infringement by Multiple Parties*, LEXOCOLGY (Nov. 30, 2011), <http://www.lexology.com/library/detail.aspx?g=86c69698-1a85-44c4-9139-192fffe6c6d5>; *Opinions and Orders Search*, U.S. CT. OF APPEALS FOR THE FED. CIR., <http://www.cafc.uscourts.gov/opinions-orders/0/all/mckesson> (last visited June 5, 2012).

⁹⁸ *Akamai*, 629 F.3d at 1315.

⁹⁹ *Id.*

¹⁰⁰ U.S. Patent No. 6,108,703 col.5 ll.23–27 (filed May 19, 1999).

service that delivers the base document of a web site from a content provider's computer while individual embedded objects of the website are stored on an object-by-object basis on a Content Delivery Network ("CDN").¹⁰¹ The process of "modifying an embedded object's URL to link to an object on the CDN is referred to as 'tagging.'"¹⁰²

Akamai accused Limelight, a CDN services competitor, of infringing the claims of its patents. It was, however, "undisputed that Limelight does not itself perform every step of the asserted claims."¹⁰³ Specifically, the content provider performs the "tagging" step.¹⁰⁴ Thus, Akamai relied on the joint infringement theory in its arguments and contended that Limelight had necessary "direction or control" as defined in *BMC* because Limelight "contractually requires content providers to perform the tagging."¹⁰⁵ In ruling in favor of Limelight, the Federal Circuit extended the "direction or control" standard by adding that two separate parties need to have an "agency relationship" or a "contractual obligation" in order to jointly infringe a patent claim.¹⁰⁶

The Federal Circuit later granted en banc review of the decision in order to answer the question: "if separate entities each perform separate steps of a method claim, under what circumstances would that claim be directly infringed and to what extent would each of the parties be liable?"¹⁰⁷

In their appeal brief, Akamai turned to common tort law doctrine and argued that "there is no basis . . . for ignoring . . . common law principals of torts and restricting infringement of a method claim to the conduct of a single actor, and there is certainly no support for limiting liability of joint direct infringement to a narrow, rigid agency or contractual relationship."¹⁰⁸ According to Akamai, the "doctrine of vicarious liability, based on common tort law principles and supported by precedent, provides a sensible, workable standard" as well as a "flexible fact-based" standard that avoids bright line rules.¹⁰⁹

Akamai argued that a "flexible fact-based" standard is consistent with Supreme Court Policy by pointing out that the Supreme Court has rejected "rigid" and "bright line" rules in its recent decisions in *KSR Int'l*, *Bilski*, *eBay*, and *Pfaff*.¹¹⁰ Akamai also contends that applying such a "flexible fact-based" standard would be an "effective remedy" for closing "loopholes" in which counsel attempt to "structure language of contracts so that no mastermind exists in order to avoid infringement liability."¹¹¹

Limelight, on the other hand, argued that "the standard articulated . . . in *BMC Resources* and *Muniauction* . . . is correct" and that "to permit attribution of conduct

¹⁰¹ *Akamai*, 629 F.3d at 1315.

¹⁰² *Id.* at 1316.

¹⁰³ *Id.* at 1317.

¹⁰⁴ *Id.*

¹⁰⁵ *Id.* at 1318.

¹⁰⁶ *Id.* at 1320.

¹⁰⁷ Apr. 20, 2011 Order at 2, *Akamai Tech., Inc. v. Limelight Networks, Inc.*, 629 F.3d 1311 (Fed. Cir. 2010) (Nos. 2009-1372, 1380, 1416, 1417).

¹⁰⁸ Brief for Plaintiff-Appellant on Rehearing En Banc at 3, *Akamai Tech., Inc. v. Limelight Networks, Inc.*, 629 F.3d 1311 (Fed. Cir. 2010) (Nos. 2009-1372, 1380, 1416, 1417), 2011 WL 2822716.

¹⁰⁹ *Id.* at 6.

¹¹⁰ *Id.* at 30–31.

¹¹¹ *Id.* at 33.

in the absence of direction or control would . . . conflict with and undermine . . . Congress.”¹¹² Limelight adds that Akamai’s proposed changes are “dramatic” and would expand “liability for direct infringement to reach conduct that has never before been prohibited.”¹¹³ Limelight pointed out that “the Supreme Court has held that, the courts “should be weary about looking outside of the statute itself to expand the scope of liability, lest they accurately be accused of legislating from the bench.”¹¹⁴

2. McKesson Technologies v. Epic Systems

The McKesson patent at issue is directed to “an electronic method of communication between healthcare providers and patients involving personalized web pages for doctors and their patients.”¹¹⁵ The system “facilitates direct communication between patients and their doctors” which “offers the patient significantly more information than he/she could have absorbed during a typical visit with the physician.”¹¹⁶

Epic Systems develops MyChart, a software that “allows healthcare providers to associate medical records with a patient’s personalized web page” and also “allows the patient to communicate with their healthcare providers online” through these personalized web pages.¹¹⁷ Epic Systems does not use MyChart, however. It licenses MyChart to healthcare providers, who then offer the product to their patients. If a patient uses MyChart, “that patient ‘initiates a communication’ to the provider by logging on to the healthcare provider’s MyChart web page.”¹¹⁸ Importantly, the claim is directed to “initiating a communication by one of the plurality of users to the provider” as well as several steps for processing the communication.¹¹⁹

McKesson and Epic agree that “no single party performs every step of the asserted method claims.”¹²⁰ The Court ruled that because “users acted principally for their own benefit and under their own control,” “McKesson has identified no viable legal theory under which the actions of MyChart users may be attributed to Epic’s customers. Without an agency relationship or contractual obligation, the MyChart users’ actions cannot be attributed to the MyChart providers, Epic’s customers.”¹²¹ The Federal Circuit thus affirmed the district court’s non-infringement ruling.¹²² In

¹¹² Brief of Defendant Cross-Appellant on Rehearing En Banc at 14, 18, Akamai Tech., Inc. v. Limelight Networks, Inc., 629 F.3d 1311 (Fed. Cir. 2010) (Nos. 2009-1372, 1380, 1416, 1417), 2011 WL 3796785.

¹¹³ *Id.* at 41.

¹¹⁴ *Id.* at 41–42.

¹¹⁵ See *McKesson Tech., Inc. v. Epic Sys. Corp.*, 2011 WL 1365548, at *2 (Fed. Cir. Apr. 12, 2011).

¹¹⁶ *Id.*

¹¹⁷ *Id.* at *3.

¹¹⁸ *Id.*

¹¹⁹ *Id.* at *4.

¹²⁰ *Id.* at *6.

¹²¹ *Id.* at *8.

¹²² *Id.* at *11.

other words, simply providing software to a party, or even encouraging the party to use the software, is not enough to establish “direction or control.”¹²³

The Federal Circuit later granted en banc review of the decision in order to answer the questions: “if separate entities each perform separate steps of a method claim, under what circumstances, if any, would either entity or any third party be liable for inducing infringement or for contributory infringement” and “does the nature of the relationship between the relevant actors—e.g., service provider/user; doctor/patient—affect the question of direct or indirect infringement liability?”¹²⁴

In their appeal brief, McKesson, like Akamai, argued that the Court should look to “tort-related” principals in answering questions related to joint infringement since the Patent Act does not expressly answer [the] court’s questions.”¹²⁵ McKesson argued that, even though the *BMC* line of cases correctly acknowledged tort law doctrine by adopting a “direction or control” standard, the Federal Circuit “erred in effectively converting the ‘direction or control’ test into a ‘control’ one and limiting liability to only two forms of control: an agency relationship or contractual obligation.”¹²⁶ Instead, McKesson suggested a broader test in which “one party’s conduct is attributed to another if the other directed, controlled, induced, or failed to exercise a right to control that conduct.”¹²⁷

Epic, like Limelight, argued that in *BMC* and *Muniauction*, the Federal Circuit “properly interpreted the 1952 Patent Act” in requiring “a showing of agency or contractual obligation for direct infringement of a method claim where the steps of the method are performed by more than one actor.”¹²⁸ Epic argued that McKesson’s suggestion to expand direct infringement doctrine to “encompass all possible historical state common-law rules for finding multiple parties liable no matter the context in which those rules were developed . . . stretches the rule” beyond what the Supreme Court intended in *Meyer v. Holley*.¹²⁹

F. Amici Support and Opposition for Akamai and Limelight

The American Intellectual Property Law Association (“AIPLA”) agrees that an “analysis should not require an agency relationship between the parties who perform the method steps or a contractual obligation” but instead “should conform to the traditional tort law basis for patent infringement.”¹³⁰ As *Akamai* did, the AIPLA also points out that the current law has “created a gaping loophole that renders issued and future patents in important technologies virtually unenforceable” and that

¹²³ *Id.* at *8, 10–11.

¹²⁴ Opening En Banc Brief of Plaintiff-Appellant at 3, *McKesson Tech., Inc. v. Epic Sys. Corp.*, 495 F. Supp. 2d 1329 (N.D. Ga. 2007) (No. 2010-1291), 2011 WL 2822667.

¹²⁵ *Id.* at 17.

¹²⁶ *Id.* at 27.

¹²⁷ *Id.* at 26.

¹²⁸ Defendant-Appellee’s Response at 28–29, *McKesson Tech., Inc. v. Epic Sys. Corp.*, 495 F. Supp. 2d 1329 (N.D. Ga. 2007) (No. 2010-1291), 2011 WL 3796780.

¹²⁹ *Id.* at 33–34.

¹³⁰ Amicus Brief of Am. Intell. Prop. Law Ass’n in Support of Neither Party at 4, *McKesson Tech., Inc. v. Epic Sys. Corp.*, 495 F. Supp. 2d 1329 (N.D. Ga. 2007) (No. 2010-1291) 2011 WL 3101832.

unless corrected, the current law “encourages development of business models designed to misappropriate the patented methods of others.”¹³¹

The Electronic Frontier Foundation, however, sides with Limelight and Epic and argues that changing the current law “would create a new category of potential patent defendants” that are likely “to lack both requisite knowledge of the patent laws and resources to make a robust defense” resulting in these persons taking on “risk that they never contemplated and would be hard pressed to mitigate.”¹³²

G. What Will the Federal Circuit Do?

During oral arguments, the Federal Circuit thoroughly questioned each side, posing hypotheticals that pointed out weaknesses in each side’s suggested approach to the joint infringement doctrine.¹³³ Although this may simply be an indication of the Federal Circuit taking a neutral ground and keeping an open mind during oral arguments, it may also be an indication of difficult challenge the court faces. On the one hand, the Federal Circuit may choose to close existing loopholes by turning to tort law and eliminating the single entity standard and the need for the “direction or control” test. This decision, however, may expose a whole new set of potential defendants to patent litigation, unfairly in some cases.¹³⁴ On the other hand, the Federal Circuit may choose to closely follow precedent and keep the standard as is. This decision, however, may enable would-be infringers to otherwise continue to unfairly practice methods of a claimed invention.¹³⁵ Alternatively, the Federal Circuit may chose to maintain the current single entity standard but to soften the associated rigid “direction or control” standard.¹³⁶ For example, the court may choose to address and clarify the types of relationships that may result in necessary “direction and control.”¹³⁷

So what will the Court do? First, it is unlikely that the Federal Circuit will do anything dramatic. The Federal Circuit has repeatedly shown an unwillingness to deviate substantially from the status quo with respect to patent rules, without legislative direction. Here, in particular, where joint infringement problems can theoretically be avoided with appropriate claim drafting techniques, the court is less likely to make substantial changes to the joint infringement doctrine.

¹³¹ *Id.*

¹³² Amicus Brief of Elec. Frontier Found. In Support of Defendant at 2, *McKesson Tech., Inc. v. Epic Sys. Corp.*, 495 F. Supp. 2d 1329 (N.D. Ga. 2007) (No. 2010-1291) 2011 WL 4439012.

¹³³ Oral Argument Recording: *Akamai Tech. v. Limelight Networks*, available at <http://www.cafc.uscourts.gov/oral-argument-recordings/2009-1372/2011-11-18/all>; see also H. Wayne Porter, *Patent Law Update: Akamai and McKesson Oral Arguments*, BANNER & WITCOFF, LTD. (Nov. 21, 2011), <http://www.bannerwitcoff.com/news/749/>.

¹³⁴ See *supra* Part II.D, and accompanying text.

¹³⁵ *BMC Res., Inc. v. Paymentech, L.P.*, 498 F.3d 1373, 1381 (Fed. Cir. 2007); Kristin E. Gerdelman, *Subsequent Performance of Process Steps by Different Entities: Time to Close Another Loophole in U.S. Patent Law*, 53 EMORY L.J. 1987, 2012 (2004) (“The separate entities loophole allows, and even encourages, clever infringers.”).

¹³⁶ See *supra* Part II.B, and accompanying text.

¹³⁷ See, e.g., *Akamai Tech., Inc. v. Limelight Networks, Inc.*, 629 F.3d 1311, 1320 (Fed. Cir. 2010) (explaining that joint infringement can only be found “when there is an agency relationship” or “when one party is contractually obligated to the other”).

Nevertheless, the Court is also equally unlikely to maintain status quo. The existing joint infringement doctrine may provide potential infringers an opportunity to—some would argue, unfairly—escape liability.¹³⁸ The Federal Circuit’s decision to review the two opinions is also an indication that the court itself sees problems with the existing doctrine and a potential opportunity to improve the doctrine.

Thus, while the Federal Circuit is likely to maintain the “direction or control” standard for joint infringement, at the same time, the court is likely to soften the “mastermind” standard. Specifically, the Federal Circuit may expand the types of relationships that may constitute proper “direction or control.” In other words, the Federal Circuit may attempt to close the loophole in the current standard without extensively deviating from the current standard.

H. Cloud Computing Claims After Akamai and Limelight

In the unlikely event that the Court dramatically changes the current joint infringement doctrine and eliminates the single entity rule, there would be a significant shift in strategy for drafting cloud computing claims. In particular, it would become advisable to draft claims covering actions of multiple parties in a cloud computing system.¹³⁹ For example, rather than worrying about whether a single actor/corporation is likely to infringe the claims, a cloud computing company could benefit from anticipating possible relationships of multiple potential infringers and then draft claims to cover the actions of all parties. Thus, a cloud computing company could position itself for targeting multiple defendants instead of targeting just one. This could come with a price, however. A cloud computing company could just as easily become exposed as a defendant itself, under such new rules. For example, a cloud computing company that offers a single service that interfaces with, and is utilized by, a second service offered by a second service provider may be accused of infringing a cloud computing claim that is directed to the steps performed by both services providers in combination.¹⁴⁰

In the event that the Federal Circuit decides to keep the joint infringement doctrine as is, with little or no change, cloud computing companies would similarly see little change in the way they go about protecting their intellectual property and defending against infringement accusations. Mainly, cloud computing companies would continue to attempt to draft claims from the perspective of a single entity.¹⁴¹ While the current doctrine would continue to make it difficult for the cloud computing companies to enforce claims that are jointly infringed, the current doctrine would also make it equally easy for the companies to avoid joint infringement allegations by exploiting existing loopholes.¹⁴²

In the event that the Federal Circuit decides to implement a “softer” version of the current “direction or control” standard, cloud computing companies should take note of the change and adapt claim drafting and litigation strategies accordingly.

¹³⁸ See *BMC*, 498 F.3d at 1381.

¹³⁹ See *supra* Part II.C, and accompanying text.

¹⁴⁰ *Id.*

¹⁴¹ See Helmsen & Terril, *supra* note 14, at 3.

¹⁴² See Gerdelman, *supra* note 135, at 2012.

Specifically, claim drafters should probably continue to draft core claim sets from the perspective of a single entity.¹⁴³ In addition, however, claim drafters should also get creative by anticipating certain relationships that may constitute proper “direction or control” under the new standard and draft claims directed to those relationships as well.¹⁴⁴ For example, a cloud computing company may offer an application service that interfaces with a data service. If the Federal Circuit determines that an application service provider interfacing with a data service provider, in general, constitutes proper “direction or control,” the application service provider may wish to own patent claims directed to steps performed by the service provider alone as well as patent claims directed to steps being performed by both the service provider and the data provider.¹⁴⁵ This could give the service provider more flexibility and more options when enforcing a patent.¹⁴⁶ On the other hand, cloud computing companies should also pay attention to any newly defined relationships that could potentially position them as defendants in a joint infringement claim. Specifically, cloud computing companies should be conscious of the loopholes that are being closed by a new standard but should also be conscious of loopholes that may remain open under the new standard when forming business relationships or partnerships.¹⁴⁷

Interesting to note, both *Akamai* and *McKesson* appear to be focusing on method claims alone and not on system claims.¹⁴⁸ As discussed, the Federal Circuit has taken a different approach to system claims as it has with method claims, with respect to joint infringement.¹⁴⁹ Thus, regardless of how *Akamai* and *McKesson* are decided, unless the Federal Circuit discusses system claims in particular, the approach to drafting cloud computing system claims will likely not change significantly, at least not immediately. However, any changes made should strongly be considered, even when drafting system claims. This is because, even though the Federal Circuit may be directing its current opinion to method claims in particular, in future cases, courts (including the Federal Circuit) may look to this decision for guidance when deciding joint infringement of systems claims. Accordingly, it may benefit a future holder of a cloud computing patent to have system claims that have been drafted in light of the *Akamai* and *McKesson* decisions.

III. CONCLUSION

In short, the increasing popularity and complexity of cloud computing systems requires patent claim drafters to pay close attention to the existing joint infringement doctrine. In addition, the evolving doctrine may necessitate a major

¹⁴³ See *supra* Part II.D, and accompanying text.

¹⁴⁴ See *Akamai Tech., Inc. v. MIT*, 419 Fed. Appx. 989, 989 (Fed. Cir. 2011) (ordering *en banc* hearing on issue of joint infringement).

¹⁴⁵ See *supra* Part II.D, and accompanying text.

¹⁴⁶ *Id.*

¹⁴⁷ See *supra* Part II.E, and accompanying text.

¹⁴⁸ See *Akamai Tech., Inc. v. Limelight Networks, Inc.*, 629 F.3d 1311, 1316 (Fed. Cir. 2010) (discussing patents at issue); see also *McKesson Tech. Inc., v. Epic Sys., Corp.*, 495 F. Supp. 2d 1329 (N.D. Ga. 2007) (naming patents at issue).

¹⁴⁹ See *supra* Part II.B–C, and accompanying text.

strategy shift in drafting cloud computing claims although more than likely will only drive a smaller incremental shift in how such claims are drafted.