AVOID THE RAINY DAY: SURVEY OF U.S. CLOUD COMPUTING CASELAW*

Fernando M. Pinguelo** & Bradford W. Muller***

Cloud computing, a computer networking model that gives users on-demand access to shared software applications and data storage, [1] is becoming increasingly popular among businesses and individuals. For example, if you use Google's Gmail [2] for your email and calendaring, or Snapfish [3] for your online photo sharing and storage; or if your business remotely stores data with a third-party server provider like Salesforce, [4] or uses Windows Azure [5] to create and host web applications and services, you are already "floating in a cloud." To provide guidance to those companies working within a cloud - or those considering utilizing cloud computing - this article surveys U.S. cases that have direct, substantive implications for cloud users. These cases implicate issues of personal jurisdiction, privacy rights, e-discovery, and copyright infringement. [6] We also take a brief look at the newest case on the cloud computing horizon, *Google v. The United States*. [7]

I. PERSONAL JURISDICTION: USING CLOUD COMPUTING MAY INCREASE THE POSSIBILITY THAT A COMPANY WILL HAVE TO FEND OFF A LAWSUIT IN ANOTHER STATE

In 2008, a New York trial court decided *Forward Foods LLC v. Next Proteins, Inc.*, [8] which addressed, in part, how cloud computing impacts personal jurisdiction. There, plaintiffs sued a non-domiciliary for breach of contract and fraud stemming from the sale of a food business. [9] Forward Foods was a Delaware LLC with its principal place of business in Nevada, [10] while co-plaintiff Emigrant Capital was a Delaware corporation based in New York. [11] The defendant, Next Proteins, was incorporated and headquartered in California. [12] Emigrant Capital owned ninety-four percent of Forward Foods, and decided to file the joint lawsuit in New York. [13] Next Proteins moved to dismiss the claims for lack of personal jurisdiction and forum non conveniens. [14]

The interaction between the litigants originally began when, to facilitate the sale of the food business, Next Proteins hired an outside company to establish a "virtual data room" in which Next Proteins would upload electronic documents related to their business and allow entities interested in buying the company to access the virtual room through a password. [15] Once inside, the interested buyers could download the documents. [16] Next Proteins, as the seller, gave Emigrant Capital, the buyer, a password to this virtual room, which Emigrant Capital accessed from its New York office, using the room to inspect Next Proteins' documents and perform due diligence. [17] When Emigrant Capital would request additional documents, Next Proteins would upload the information to the virtual room. [18]

The court held that Next Proteins' electronic activities had created sufficient minimum contacts with New York and that the company had "clearly transacted business within the state" such that personal jurisdiction was established. [19] However, the court granted the motion to dismiss for forum non conveniens. [20]

In its personal jurisdiction analysis, the court made note of the fact that there was "a virtual data room where Defendants uploaded documents for Emigrant to review in New York[.]" [21] This proved to be a significant factor in finding that defendants had maintained sufficient contacts with New York to be subject to personal jurisdiction. [22] However, the particular facts of this case made California the far more convenient forum, and as such the court stated that Next Proteins' New York contacts, derived in part from the virtual data room, were not sufficient to overcome the fact that California was the better location for the suit. [23]

e-Lesson Learned: [24]

It is apparent that the use of a cloud can potentially increase the number of "contacts" a party is found to have for personal jurisdiction purposes, and thus raise its exposure to lawsuits in multiple forums. Although using a cloud for collaborative purposes, such as the online storage of documents in a virtual data room, can make it easier to interface with potential clients, it does come with inherent risks. Nevertheless, the forum non conveniens doctrine [25] could protect the otherwise vulnerable cloud user from mass exposure to lawsuits in far-off jurisdictions.

II. Privacy Rights: As Judges Become More Technologically Savvy, They Will Be More Willing to Recognize The Right to Privacy for Data Stored in a Cloud

The enlightened discussion contained in a dissenting opinion in State v. Bellar [26] is heartening for any privacy-concerned company or individual currently using cloud services for off-site data storage. In this case, defendant was charged with multiple criminal counts related to child pornography found on his computer. [27] A technician found the material on the defendant's hard drive after defendant brought his computer to a repair shop. [28] The technician copied the images to a compact disc (CD), and turned the CD over to the police. [29]
The muddled procedural history of the case is irrelevant for our purposes, but the dissenting judge's opinion offers an excellent discussion of cloud computing and privacy rights. There, Judge Sercombe opined:
Nor are a person's privacy rights in electronically stored personal information lost because that data is retained in a medium owned by another. Again, in a practical sense, our social norms are evolving away from the storage of personal data on computer hard drives to retention of that information in the "cloud" of servers owned by internet service providers. That information can then be generated and accessed by hand-carried personal computing devices. I suspect that most citizens would regard that data as no less confidential or private because it was stored on a server owned by someone else. [30]

e-Lesson Learned:

There is a growing recognition among technologically savvy members of the bench that litigants have an expectation of privacy for information that they store in a cloud. As courts continue to become more computer-literate, and cloud computing gains increased mainstream recognition, it is likely that privacy rights in data saved in a cloud will be given increased protection.

III. e-Discovery: Just Because a Company Uses a Third-Party to Store Data Does Not Mean That It Will Be Exempt From Having to Turn Over Information During the "Discovery" Phase of a Trial

Moving to the realm of e-discovery, *Columbia Pictures, Inc. v. Bunnell* [31] was a copyright infringement action where plaintiff, a movie studio, brought suit against defendant, a website that enabled users to download torrent files from a peer-to-peer file sharing network, thus facilitating the online pirating of plaintiff's movies and television programs. [32] The magistrate judge had granted in part, and denied in part, Columbia Picture's motion to require Bunnell to preserve and produce its server log data. [33] On appeal to the district court, defendant argued that it could not meet the discovery demand, since it had recently employed a third-party data storage provider who did not log the data. [34]

The court found that the magistrate judge's ruling was based on sufficient evidence, thus affirming the finding that the data in issue, which was being routed to a third party entity and received in that third-party's server, was within defendant's possession, custody, or control by virtue of defendant's "ability to manipulate at will" how the data was routed. [35] Proof of defendant's ability to manipulate the data's route was found in the fact that, just one month prior to the evidentiary hearing, defendant had rerouted the data from its own servers to those of the third-party. [36] Accordingly, since defendant had the ability to reroute the server log data to itself (even if the third-party contractor could not produce such logs), the court held that the discovery ruling was adequately supported by the record. [37]

e-Lesson Learned

It is increasingly difficult for parties to hide behind their remote data storage providers when fielding e-discovery requests, as courts find those servers to be within the party's "possession, custody or control." Similarly, in *Tomlinson v. El Paso Corporation*, [38] the district court held that an employer was in possession, custody, or control of digital pension plan data and other documentation held by a third-party record-keeper; and thus the employer could be compelled to produce the data and documentation. [39]

IV. Copyright Infringement: Depending on the Circumstances, How a Company Uses its Cloud Could Infringe on the Copyrights of Others

As for the fertile realm of copyright infringement, in *Cartoon Network v. CSC Holdings, Inc.*, [40] owners of copyrighted programming brought an action against a cable television company, Cablevision, seeking a

declaratory judgment regarding whether Cablevision's cloud-based remote storage digital video recorder system, more commonly known as an "RS-DVR," violated their respective copyrights, and sought an injunction preventing Cablevision from rolling out the RS-DVR technology without copyright licenses from the content providers. [41] The district court granted summary judgment in favor of the copyright owners, and Cablevision appealed. [42]

The Second Circuit found that the RS-DVR technology did not directly infringe on the content providers' copyrights, and accordingly reversed the summary judgment and vacated the injunction. [43] The court reasoned that the data which contained the copyrighted programs, and which was moved to "buffers" to allow customers to record the program on the RS-DVR, only remained in the buffers for a very short period of time, a mere 1.2 seconds, and was automatically overwritten as soon as it was processed, such that the data was not "fixed" as is required to qualify as a "copy" under the Copyright Act. [44] Additionally, the copies of the programs were "made" by the customer, since they were created upon the customer's demand, and therefore Cablevision's contribution to the reproduction by providing the RS-DVR did not warrant imposition of direct liability under the Copyright Act. [45] And finally, the court found that when a customer plays a copy of a recorded program for his or her personal enjoyment, that does not qualify as a performance "to the public," and therefore it did not violate the exclusive right of performance under the Copyright Act. [46]

e-Lesson Learned:

This remains a topical issue that could see its day in the Supreme Court, as certiorari was denied, in part, because the Solicitor General found that the RS-DVR technology needed more time to develop. [47]
As seen in Cartoon Network, a litigant may attempt to argue that copyright infringement occurred as the result of a company's or individual's actions within a cloud. Like file-sharing websites who operated without the permission of the copyright owners of the content they shared, companies or individuals who use a cloud to make unauthorized content available to Internet users may expose themselves to liability for copyright infringement. Although the cable provider in Cartoon Network was able to escape liability in part because of the unique attributes of the RS-DVR technology, not every defendant is so lucky.

For example in *Arista Records, LLC v. Usenet.com, Inc.*, [48] recording companies brought a copyright infringement action against the defendant, UCI, for operating a file distribution service which made copyrighted music available for download. [49] The cloud at issue here was the USENET Network, "a global system of online bulletin boards" on which subscribers could post their own messages or files and download files posted by others. [50] The district court granted plaintiffs' motion for summary judgment, finding, among other things, that defendants actively promoted direct copyright infringement, [51] and that they intended to induce or foster copyright infringement by the cloud's users. [52] The court's reasoning was based, in part, on the fact that it found "rampant" evidence of copyright infringement occurring on the USENET, and undisputed evidence that copyrighted sound recordings had been uploaded to the cloud and downloaded by users. [53] Furthermore, former UCI employees "testified that their marketing department had specifically targeted young people familiar with other file-sharing programs[.]" [54]

e-Lesson Learned:

The lesson here is simple: If there is any company left which has not learned from Napster, [55] this case makes clear that copyright infringement will not be tolerated in the peer-to-peer file sharing realm. Simply because the copyright infringement is by way of a download, rather than buying a bootleg copy of a CD from a street vendor, does not make it any less illegal or harmful to the copyright holder.

V. CLOUD WARS: PROVIDERS SUCH AS MICROSOFT AND GOOGLE ARE FIERCELY COMPETING TO OFFER CLOUD COMPUTING SERVICES

In what is undoubtedly a sign of things to come, Google and Microsoft are now battling for dominance in the cloud computing services market. In *Google v. The United States*, recently filed in the U.S. Court of Claims, the Department of Interior (DOI) was seeking a cloud service provider to outfit the agency with a "single hosted email and collaboration services solution" in an effort to centralize their messaging system, which currently includes thirteen separate email platforms. [56] Google believed that it could present a competitive offer with its Google Apps product, [57] "the first suite of cloud-computing messaging and collaboration applications to receive [Federal Information Security Management Act (FISMA)] certification and accreditation." [58] But according to Google, despite repeated efforts at conveying their interest and the abilities of their cloud-product, the DOI information

technology team was focused on moving forward with a new Microsoft cloud-service, Business Productivity Online Suite-Federal (BPOS). [59] Google claims that the Microsoft BPOS product is new and untested, as it has not been certified to meet FISMA standards. [60] Google also claims that the DOI's insistence on a "private cloud" for the Department, i.e. "that the messaging solution's data storage and computing infrastructure be physically and logically dedicated only to Federal government customers," was not necessary to satisfy the Department's needs. [61]
Believing that the seemingly pre-determined decision to move forward with Microsoft's BPOS was in violation of federal law, Google now seeks to enjoin the DOI from continuing to proceed with its placement process, and asks for an order requiring the DOI to hold an open and competitive bid process in accordance with the Competition in Contracting Act, 41 U.S.C. 253(a). [62]

With the market for cloud-based solutions on the rise, this is sure to be just one of many "cloud wars." As competition increases among cloud service providers, customers will likely benefit from more affordable pricing rates and dramatic technological advances. [63]

VII. CONCLUSION

Cloud computing remains a relatively new technology that will generate a variety of legal issues as time goes on. In the meantime, cloud-users should heed the lessons learned from early court decisions, and avoid the pitfalls of their predecessors. While the cloud can be a tremendous business tool, only time will tell how courts will perceive its use in terms of privacy rights, [64] personal jurisdiction, and other important issues. It is hoped that these future decisions will help to advance technology while at the same time respecting the legal rights of those impacted by the use of cloud computing.

* Preliminary version of article presented on November 5, 2010 at the American Bar Association - International Law Section Annual Meeting, Paris, France.

** Fernando M. Pinguelo, a Partner at Norris, McLaughlin & Marcus, P.A. and co-Chair of its Response to Electronic Discovery & Information Group, is a United States-based trial lawyer who devotes his law practice to complex business lawsuits with an emphasis on how technology impacts them. He has lectured internationally and written dozens of articles on the topic. He works closely with business owners and executives to develop strategies to manage business and legal issues related to electronic documents. As an adjunct professor at Seton Hall University School of Law, Mr. Pinguelo has developed and teaches a state-of-the-art course on eDiscovery and how technology impacts lawsuits. Recently, the U.S. Fulbright Program designated him a Fulbright Specialist for his work in eDiscovery; and he will guest lecture at Mackenzie University, São Paulo, Brazil next year. Mr. Pinguelo also founded and contributes to the ABA Journal Award-winning blog, eLessons Learned - Where Law, Technology, & Human Error Collide. To learn more about Mr. Pinguelo, visit www.NJLocalLaw.com or email him at info@NJLocalLaw.com.

*** Bradford W. Muller, an Associate at Norris, McLaughlin & Marcus, P.A., is a graduate of Seton Hall University School of Law, magna cum laude, where he was a Comments Editor on the Seton Hall Law Review. Prior to his current position, Mr. Muller was a Judicial Law Clerk to the Honorable Anthony J. Parrillo, New Jersey Superior Court, Appellate Division.

[1]. Peter Mell & Tim Grance, *The NIST Definition of Cloud Computing*, Oct. 7, 2009, *available at* http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc.

[2]. *Gmail: Email from Google*, https:// www.google.com/accounts/ServiceLogin? service=mail&passive=true&rm=false&continue=http%3A%C2F%C2Fmail.google.com%C2Fmail%C2F%C3Fui% C3Dhtml%C26zy%% 3Dl&bsv=1eic6yu9oa4y3&scc=1&ltmpl=default&ltmplcache=2 (last visited Dec.3, 2010).

[3]. *Snapfish by HP*, http://www.snapfish.com/snapfish/welcome (last visited Dec. 3, 2010).

[4]. *Salesforce.com*, https://www.salesforce.com/form/sem/crmdemo_opt2.jsp? d=70130000000FT7m&DCMP =KNC-MSN&mkwid=t3qJKpV7&pcrid=174921462 (last visited Dec. 3, 2010).

[5]. *Online Collaboration, Productivity Tools, Microsoft Cloud Power*, http://www.microsoft.com/en-us/cloud/cloudpowersolutions.aspx?CR_ CC=200010705&WT.srch=1&WT.mc_id=CCDDCC16-7319-4FCE-9B03-DA863B65F0EA&CR_ SCC=200010705 (last visited Dec. 3, 2010).

[6]. As of the date of this publication, these cases represent the list of known case-law that most directly impacts cloud computing substantively. For an expanded discussion of other case-law related to the cloud and current trends in cloud computing, see Mark H. Wittow, CLOUD COMPUTING: RECENT CASES AND ANTICIPATING NEW TYPES OF CLAIMS (in Cloud Computing 2010, Practicing Law Institute, March 2010) (available on Westlaw); see also David D. Cross & Emily Kuwahara, *E-Discovery and Cloud Computing: Control of ESI in the Cloud*, 1 EDDE JOURNAL 2 (2010) *available at* http://www.crowell.com/documents/E-Discovery-and-Cloud-Computing-Control-of-ESI-in-the-Cloud.pdfF.

[7]. For an online version of the complaint, visit http://ellblog.com/wp-content/uploads/2010/11/Google-v-US-Dept-of-Interior-CFC-10-743-complaint.pdf

[8]. 2008 BL 238516 (N.Y. Sup. 2008).

[9]. *Id.* at *1.

[10]. *Id.*

[11]. *Id.*

[12]. *Id.*

[13]. *Id.*

[14]. Forward Foods LLC, 2008 BL 238516 at *1.

[15]. *Id.*

[16]. *Id.*

[17]. *Id.*

[18]. *Id.*

[19]. *Id.* at *3.

[20]. Forward Foods LLC, 2008 BL 238516 at *4.

[21]. *Id.* at *3.

[22]. *Id.*

[23]. *Id.* at *4.

[24]. For more e-lessons, visit e-Lessons Learned - Where Law, Technology, & Human Error Collide at www.ellblog.com. E-Lessons Learned, an educational blog about e-discovery, technology, and human error, features insightful content authored primarily by law students from across the country. e-Lessons Learned designs its posts to appeal to a broad spectrum of readers. Each blog post: (a) identifies cases that address technology mishaps (either through negligence, ethical lapses in judgment, too much reliance on outside counsel and vendors, or fraud); (b) exposes the specific conduct that caused a problem; (c) explains how and why the conduct was improper; and (d) offers suggestions on how to learn from these mistakes and prevent similar ones from reoccurring.

[25]. "The doctrine of forum non conveniens is a common law principle that gives courts the discretion to decline exercising jurisdiction over certain cases where the underlying principles of justice and convenience favor dismissal." Helen E. Mardirosian, *Forum Non Conveniens*, 37 LOYOLA LOS ANGELES L. REV. 1643, 1643 (2004).

[26]. 217 P.3d 1094 (Or. App. Sept. 30, 2009).

[27]. *Id.* at 1095.

[28]. *Id.* at 1095-96.

[29]. *Id.* at 1096.

[30]. *Id.* at 1110-11.

[31]. 245 F.R.D. 443 (C.D. Cal. 2007).

[32]. *Id.* at 445.

[33]. Id at 445-46.

[34]. *Id.* at 453.

[35]. *Id.*

[36]. *Id*.

[37]. *Columbia Pictures, Inc.*, 245 F.R.D. at 453.

[38]. 245 F.R.D. 474 (D. Colo. 2007).

[39]. *Id*. at 477.

[40]. 536 F.3d 121 (2d Cir. 2008), cert. denied, 129 U.S. 2890 (2009).

[41]. *Id.* at 123.

[42]. *Id.*

[43]. *Id.*

[44]. *Id.* at 129-30.

[45]. *Id.* at 130-34.

[46]. *Cartoon Network*, 536 F.3d at 134-40.

[47]. Wittow, *supra* note [6], at 3.

[48]. 633 F. Supp. 2d 124 (S.D.N.Y. 2009).

[49]. *Id.* at 129.

[50]. *Id.* at 129-30.

[51]. *Id.* at 148-49.

[52]. *Id.* at 151-54.

[53]. *Id.* at 131-32.

[54]. *Arista Records, LLC*, 633 F. Supp. 2d at 132-33.

[55]. *See* The Rise and Fall of Napster, May 30, 2002, http:// www.bbc.co.uk/dna/h2g2/A741089.

[56]. Complaint at ¶6, ¶33, No. 10 Civ. 00743, (Fed. Cl. Oct. 29, 2010).

[57]. *Id.* at ¶7.

[58]. *Id.* at ¶22.

[59]. *Id.* at ¶32.

[60]. *Id.* at ¶41.

[61]. Comp. at ¶13, ¶45.

[62]. *Id.* at ¶1, ¶¶51-52.

[63]. For more information on the progress of Google v. The United States, register to receive timely updates at Google Watch: http://ellblog.com/?page_ id=2179.

[64]. For the Obama administration's take on federal oversight over online privacy, see the draft report by the U.S. Department of Commerce, Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework," available at http://www.ntia.doc.gov/internetpolicytaskforce.