Chapter 8
Alternative Dispute Resolution, Litigation Strategies, and Bankruptcy Considered in the Context of Cloud Agreements

By Thomas A. Capezza and Nancy L. Urizar

I. Introduction

This chapter examines methods of resolving disputes arising with cloud computing agreements, focusing on the benefits of alternative dispute resolution clauses in Part II and preserving cloud contents as a litigation safeguard in Part III. Part IV discusses strategies to mitigate business interruption when a cloud provider declares bankruptcy.

II. The Benefits of Alternative Dispute Resolution Clauses

Alternative dispute resolution (ADR) is the use of processes or methods such as mediation and arbitration to resolve a dispute instead of litigation. As discussed more fully below, the benefits of including ADR clauses in cloud computing agreements include time and cost savings, maintaining confidentiality as to proprietary data and the ultimate outcome, and minimizing business disruption.

A. ADR Clauses Save Time, Money, and Business Relationships

ADR clauses have been shown to yield time and cost savings. In March 2013, the World Intellectual Property Organization (WIPO) Arbitration and Mediation Center (WIPO Center) conducted a survey to “assess the current use in technology-related disputes of Alternative Dispute Resolution . . . methods as compared to court litigation, including a qualitative evaluation of these dispute resolution options.” A total of 393 participants (law firms, companies, research organizations, universities, government bodies, and the self-employed) from 62 countries completed the survey; 63 of these participants, from 28 countries, complemented their written responses with a telephone interview.

1 Thomas A. Capezza is a director at Carter, Conboy, Case, Blackmore, Maloney & Laird, P.C., specializing in white-collar litigation, government investigations, and technology issues. Nancy L. Urizar is an associate at Goodwin Procter LLP. Research assistance by Kasey K. Hildonen and Claudia C. Cadenillas.

Participants reported that the duration of litigation in their home jurisdiction was on average approximately three years and cost approximately $475,000. When litigating in another jurisdiction, the corresponding numbers were three and one-half years and $850,000.3

By contrast, participants reported that mediation4 took an average of eight months, and 91 percent of participants reported that the costs of mediation typically did not exceed $100,000.5 Similarly, participants indicated that arbitration6 took a little more than one year and cost on average slightly over $400,000.7

Apart from mediation and arbitration, ADR proceedings based on expert determinations8 expedited resolution of disputes in a cost-effective manner. Participants indicated on average that expert determinations took slightly more than six months; nearly three-quarters of participants indicated that the costs of expert determination would not typically exceed $50,000.9 The efficiencies of expert determinations are all the more evident when you consider the litigation alternative—that is, the costs of retaining an expert, coupled with broader litigation costs, are higher and include persuading a judge or jury who may be unfamiliar with the subject technology. Thus, due to their technical nature, cloud-based disputes lend themselves to ADR inasmuch as experts may serve as decision makers in ADR proceedings, rather than serving as witnesses to persuade nontechnical decision makers in litigation.10 Using ADR may also reduce “wasted management time of business executives and other participants in proceedings, lost productivity, and lost business opportunities due to the reserves required to cover the worst potential outcome of a pending dispute,” which 25 percent of participants mentioned as among the costs they considered.11

ADR clauses also serve to minimize business disruption. Dispute-resolution procedures may be tailored to, among other things, the specific circumstances of the technology, the confidential or proprietary nature of the subject data, and the unique dynamics of the business relationship.12 Those procedures may serve to remove litigation altogether or mandate mediation as a precondition to litigation. Thus, even where mediation is unsuccessful, it may serve to triage and thereby narrow disputed issues, improve dialogue

---

3 WIPO Survey Results, supra note 2, at 30.
4 Mediation, as used in this context, is an “informal procedure in which a neutral intermediary assists the parties in reaching a settlement of the dispute.” Id. at 36.
5 Id. at 30.
6 Arbitration, as used in this context, is an “out-of-court procedure in which the dispute is submitted to one or more arbitrators who make a binding decision.” Id. at 36.
7 Id. at 30.
8 “Expert determination,” as used in this context, is a “procedure in which a matter is submitted to one or more experts who make a determination on the matter referred by the parties. The determination is binding, unless the parties have agreed otherwise.” Id. at 36.
9 Id. at 32.
10 WIPO Survey Results, supra note 2, at 5 (reporting that specialization of the decision maker is one of the main considerations when negotiating dispute resolution clauses); see also Cloud Computing Agreements, supra note 2, at 6 (discussing the benefit of clauses requiring disputes to be determined by an area expert).
11 WIPO Survey Results, supra note 2, at 33.
12 See Cloud Computing Agreements, supra note 2, at 2.
between the parties, minimize business disruption, maintain business relationships, and increase the chances of settlement in litigation.  

B. ADR Keeps the Process Confidential by Minimizing Discovery

As a separate benefit, ADR clauses may be crafted to limit discovery and the release of proprietary data, as well as to maintain secrecy of the ultimate outcome of the dispute. Court decisions have made clear that litigants have little ability to shield information from discovery, including electronic information, even when that information is in the possession of third parties. ADR clauses, therefore, present an opportunity to define the contours of document and data disclosure.

Cloud storage gained a special relevance following enactment of the Clarifying Lawful Overseas Use of Data Act, better known as the CLOUD Act. In a 2016 decision, the Second Circuit addressed whether extraterritorial data is properly within the ambit of a subpoena issued under the Stored Communications Act. Recently, however, legislation provided an answer with the CLOUD Act: generally, data stored outside of the United States has been deemed accessible by the U.S. government via subpoena in light of “government efforts to protect public safety and combat serious crime, including terrorism.”

Careful drafting of a cloud computing agreement to shepherd the parties to ADR instead of litigation may provide certain protections to a company against disclosure of confidential information by its cloud service provider in the event of a dispute. It is essential that contract provisions address exactly what data is stored, in what manner, and who will have access to it, as well as who will retain ownership of that data. Drafting standards regarding cloud storage are offered by the Legal Cloud Computing Association to address concerns such as location of data, retention policy, and ownership of data, among others.

C. Uncertainties of Civil Discovery under the SCA May Be Avoided with ADR

The control that ADR clauses provide over data discovery is relevant when comparing how courts are navigating the issue of cloud-stored data with Fourth Amendment rights.

13 Id.
14 Cloud Computing Agreements, supra note 2, at 5 (highlighting that ADR serves the purpose of maintaining confidentiality).
16 In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F. 3d 197 (2d Cir. 2016). Prior to enactment of the CLOUD Act, the U.S. Supreme Court granted certiorari to determine “whether, when the Government has obtained a warrant under [the Stored Communications Act], a U.S. provider of e-mail services must disclose to the Government electronic communications within its control even if the provider stores the communications abroad.” United States v. Microsoft Corp., 138 S. Ct. 1186, 1187 (2018). Due to the enactment of the CLOUD Act, the court dismissed the case in a per curiam decision stating that that “no live dispute remains. . . . This case, therefore, has become moot.” Id. at 1188.
The applicable legislation to this issue is the Stored Communications Act (SCA).\(^\text{19}\) Adopted in 1986 as part of the Electronic Communications Privacy Act,\(^\text{20}\) the SCA sought to address relatively new communications technology (such as e-mail)\(^\text{21}\) by regulating voluntary and involuntary disclosure of communications held by third-party service providers in an “electronic communication service” or “remote computing service.”\(^\text{22}\)

Subject to certain exceptions, the SCA generally prohibits service providers from knowingly divulging to any person or entity the “contents” of a communication while in electronic storage by that service or while carried or maintained on that service.\(^\text{23}\) Courts have labored with the distinction the SCA draws between electronic communication service (ECS) providers and remote computing service (RCS) providers, having established different standards of disclosure in litigation for each. An ECS provider is defined as “any service which provides to users thereof the ability to send or receive wire or electronic communications.”\(^\text{24}\) An RCS provider, by contrast, is defined as one offering, “provision to the public of computer storage or processing services by means of an electronic communications system.”\(^\text{25}\)

The significance of the distinction between ECS and RCS lies in the different criteria necessary to establish an exception to the general rule prohibiting disclosure by a third-party provider under the SCA—that is, an ECS provider is prohibited from divulging “the contents of a communication while in electronic storage by that service,” essentially prohibiting all content disclosures in civil litigation, although the definition of “content” itself is debatable.

By contrast, an RCS provider cannot divulge the content of any electronic communication that is carried or maintained, “solely for the purpose of providing storage or computer processing services.” However, the SCA protection will not apply if the provider has access for purposes “other than storage or computer processing.”\(^\text{27}\) This language is illustrated in situations where a cloud user consents to receiving targeted advertisements when signing up to use a free cloud service. “By sharing their data with the cloud provider, users make possible the advertising services that pay for the costs associated with providing the cloud service . . . .”\(^\text{28}\) Based on this practice, some argue that a cloud provider


\(^{20}\) Ilana R. Kattan, Note, Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud, 13 VAND. J. ENT. & TECH. L. 617, 619 (2011).

\(^{21}\) Id. at 627.

\(^{22}\) 18 U.S.C. § 2701 et seq.

\(^{23}\) 18 U.S.C. § 2702(a)(1)–(2).


\(^{25}\) 18 U.S.C. § 2711(2). “Electronic communications system” is defined as “any wire, radio, electromagnetic, photooptical or photoelectric facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.” 18 U.S.C. § 2510(14).

\(^{26}\) 18 U.S.C. § 2702(a)(1); Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 973 (C.D. Cal. 2010). “Electronic storage” is “(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” 18 U.S.C. § 2510(17).


Alternative Dispute Resolution, Litigation Strategies, and Bankruptcy

(which provides an RCS) is permitted by contract to access its users’ content in order to create user-specific advertising.29

If an RCS provider is permitted access to user information for advertising purposes, such information would not be protected by the SCA, allowing the provider to divulge the contents to the government in response to a subpoena.30 This is an important distinction between ECS and RCS providers in terms of discovery in litigation: if the cloud provider is found to be an RCS provider, the customer data it holds may be outside the scope of SCA protections.31

The distinction between ECS and RCS providers has evaded courts across the circuits, preventing them from consistently applying the principles of, among other areas, discovery and document production. This is particularly problematic when a given provider begins its service to a client as an ECS provider, but later through the retention of materials becomes an RCS provider. Thus, critics have clamored for legislative amendment that would eradicate this distinction and the disparate treatment.

This brief examination of just one complex issue that arises in litigation involving cloud-stored data and the potential for disclosure of confidential information speaks volumes to the importance of considered drafting of such agreements. When negotiating and drafting cloud-computing agreements in general, and ADR clauses in particular, the parties must determine whether communications are covered by the SCA and what type of service provider maintains the communication. “In mediation, there is generally no discovery of participants or witnesses. Further, a confidentiality clause can be drafted to require the arbitration or mediation itself to be confidential in order to avoid negative publicity for corporations.”32

A more difficult question currently the focus of the courts, however, is what protections are afforded when a party to an action subpoenas communications directly from the third-party provider. As noted by numerous courts and commentators, section 2702 of the SCA lacks any language that explicitly authorizes a service provider to divulge the contents of a communication pursuant to a subpoena or court order.33 Taking into consideration the above-discussed complexities as to what information is considered protected under the SCA, as well as the case law in this area, companies should be aware that simply storing their information with a third-party provider will not necessarily shield that information from discovery. A third-party provider can likely share the metadata without

31 Additionally, the provider of an RCS may divulge the contents of a communication with the “lawful consent” of the subscriber to the service, whereas the provider of an ECS may divulge such a communication only with the “lawful consent of the originator or an addressee or intended recipient of such communication.” 18 U.S.C. § 2702(b)(3). For instance, one of Dropbox’s main utilities is storage of information, which categorizes this service as RCS. However, if a user chooses to share a Dropbox link to another person, this communication now becomes ECS. Eric R. Hinz, Note, A Distinctionless Distinction: Why The RCS/ECS Distinction in the Stored Communications Act Does Not Work, 88 Notre Dame L. Rev. 489, 515 (2012).
32 See Cloud Computing Agreements, supra note 2, at 5.
33 See, e.g., In re Subpoena Duces Tecum to AOL, LLC, 550 F. Supp. 2d 606, 611 (E.D. Va. 2008) (“[T]he statutory language of the [SCA] does not include an exception for the disclosure of electronic communications pursuant to civil discovery subpoenas.”).
violating the SCA, and furthermore, as illustrated below, information considered in the control of a party to an action will generally be found discoverable under Fed. R. Civ. P. 26(b)(1), regardless of whether it is stored on a third-party server.

In *Flagg v. City of Detroit*, a notable and oft-cited case, the plaintiff served defendants (the city and its employees) with two subpoenas. Plaintiff sought discovery of information that supported his allegations of an inadequate investigation of his mother’s murder. The defendants argued that the SCA “wholly precludes the production in civil litigation of electronic communications stored by a non-party service provider.” SkyTel, Inc. was the nonparty service provider contracted to provide text-messaging services to the city and its employees. The services ended in 2004, but SkyTel remained in possession of the text messages. The court analyzed SkyTel’s role as a nonparty provider and concluded that the archive was maintained as “computer storage,” which defines the SkyTel service as an RCS and thus outside of the scope of the SCA protections and open to discovery requests. Given that the court found the city was still in legal control of the text messages, however, the court concluded that the straightforward solution in this case was for the plaintiff to prepare and serve a Rule 34 request to compel the city (instead of SkyTel under an SCA motion) to provide the information.

This case illustrates that courts have not yet decided whether the SCA prohibits a non-party service provider (e.g., cloud providers) from divulging contents stored for the customer. A well-written ADR clause can help one avoid such uncertainty and subsequently a FRCP 34 motion in litigation by safeguarding the confidentiality of the materials involved. The complexities of the SCA, evolving cloud technology, lagging legislation, and the court rulings in this uncertain arena make the point that ADR clauses in cloud computing agreements are a viable, if not necessary, option to ensure preservation of confidential and proprietary data.

Cases attempting to interpret the SCA expose the risks to civil litigants of broad discovery rulings. In those cases, courts have endeavored to balance the growing trend toward cloud-stored data with rights conferred by the SCA in the context of discovery during civil litigation. Due to significant progress, courts have struggled with the application of discovery production principles to cloud-computing systems. As seen above, ADR offers a way to regain control over these discovery principles.

---

35 *Id.* at 351.
36 *Id.* at 347 (emphasis added).
37 *See id.* at 363.
38 It should be noted that these facts led the court to determine that SkyTel had ceased to be an active provider of text messaging services, although it continued to maintain a database of text messages sent. The district court found that it had become an RCS provider because it served in the capacity of a “virtual filing cabinet” for the city. *Id.* at 347–48, 361.
39 *Id.* at 366.
41 *See Eric Johnson, Note, Lost in the Cloud, 69 STAN. L. REV. 867, 900 (2017).*
42 The SCA does not merely absolve a service provider from responding to a request for covered communications, it also affirmatively prohibits disclosure and authorizes a civil action against the provider for unauthorized disclosure. In some cases, a party who acquires protected communications through a subpoena could even be exposed to sanctions and liability in a civil suit if the party acquires protected communications through an improper subpoena. *See Theofel v. Farey-Jones*, 359 F.3d 1066, 1074–75 (9th Cir. 2004) (reversing a dismissal of an SCA claim). Recognizing the strength of the protections under the SCA, courts in some cases have granted a party’s motion to quash subpoenas to nonparty service providers. *Id.* at 1071–72.
D. ADR Allows a Choice-of-Law Clause

Further, ADR clauses in cloud computing agreements should include a choice-of-law provision; such clause is referred to as the “seat of arbitration.” The law that governs the agreement as a whole does not necessarily govern mediation and arbitration; therefore, the seat of arbitration, or governing law, must be specified. Forum selection, jurisdiction, and governing law clauses are essential for cloud computing agreements in that these agreements deal with products, services, and users that often span multiple jurisdictions. Choice-of-law clauses will lead to increased certainty and enforceability, and avoid costly and lengthy litigation with uncertain outcomes.

E. Limitations on ADR

There are limits to ADR clauses, however. When drafting ADR clauses, parties must be mindful of local laws that may not be waived by ADR agreements. These include, but are not limited to, laws designed to protect local business and consumers, such as obligatory warranties, import and customs, dealer protection, criminal laws, as well as bankruptcy and insolvency. For example, in America Online, Inc. v. Superior Court, a California appellate court voided forum selection and choice-of-law clauses that would have moved the case to Virginia and applied Virginia law. The California court reasoned that the clauses violated California public policy inasmuch as California consumers would have been denied protections under the California Consumers Legal Remedies Act.

Valid forum-selection clauses, however, will generally be upheld by U.S. courts unless the agreed-upon forum is inappropriate or contrary to public policy; only under extraordinary circumstances will such a provision be overridden. AT&T Mobility LLC v. Concepcion is an example of a court finding that federal law preempts a state rule that declared an arbitration clause to be against public policy. In AT&T, the plaintiffs purchased mobile services that advertised an offer of free phones; yet, they were still charged $30.22 in sales taxes. A complaint was filed and later turned into a putative class action alleging that AT&T engaged in false advertising and fraud. AT&T moved to compel arbitration under the terms of the service contract, which did not allow class-wide arbitration. The Supreme Court cited section two of the Federal Arbitration Act (FAA), which states arbitration clauses are generally “valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract.” The court refers to the

43 Cloud Computing Agreements, supra note 2, at 3.
44 E. Casey Lide, Note & Comment, ADR and Cyberspace: The Role of Alternative Dispute Resolution in Online Commerce, Intellectual Property and Defamation, 12 Ohio St. J. on Disp. Resol. 193, 200 (1996) (“Parties can develop arbitration agreements which stipulate their choice of law, eliminating potential delays which may result from a dispute over jurisdiction.”).
45 See Cloud Computing Agreements, supra note 2, at 9.
49 Id. at 337.
50 Id.
51 Id.
52 Id. at 339 (citing 9 U.S.C. § 2) (emphasis added).
italicized language as “the saving clause,” and concluded that class arbitration is inconsistent with the FAA. 53

In sum, considering the many benefits of ADR clauses and the complexities they address, cloud computing agreements should contain express ADR language.

III. Preserving Cloud Contents as a Litigation Safeguard

In those instances where ADR is not pursued or is unsuccessful, and the parties find themselves in litigation, there are a number of strategies of which a litigant should be mindful. The strategies presented below allow individuals to comply with their responsibilities as a litigant and avoid sanctions for inadequate care of evidence.

As has already been established, litigants have a duty to comply with information requests, including government and private-party subpoenas and discovery rules for anticipated, pending, or active litigation. 54 Moreover, these responsibilities are complicated by multijurisdictional and extraterritorial data storage and transfer. Again, whether a warrant issued pursuant to the SCA 55 may compel an e-mail service provider to disclose e-mails held on servers outside the United States has been debated by federal courts of different circuits with varying results and concluded with the enactment of the CLOUD Act.

A. Brief History of Cloud Storage Litigation

As mentioned above, in In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 56 initially the Second Circuit significantly narrowed the application of discovery principles relative to electronically stored information. The court denied 57 the government’s application to enforce warrants to obtain e-mail information stored outside of the country by Microsoft. The court reasoned that American courts do not have such authority because it is presumed that the SCA’s reach is limited to the borders of the United States. 58 As such, the government conceded that the SCA does not contemplate extraterritorial application. 59

53 The actual question in the case was whether FAA section two preempted California’s Discover Bank rule, which classifies most collective arbitration waivers in consumer contracts as unconscionable. The court held that the Discover Bank rule was preempted because class arbitration is poorly suited to tend to the higher stakes of litigation. See id.


56 829 F.3d 197 (2d Cir. 2016).

57 The Court of Appeals decision in this case is even more impactful on the application of discovery principles in cases involving electronically stored information (ESI). Indeed, unlike the parties in Flagg, the party demanding the information in Microsoft was the U.S. government, which has generally been given greater access under the SCA and under legal precedent. Id.

The concurrence pointed out that the decision to limit the scope of the warrant resulted from an outdated law, not a choice by Congress to hamstring investigations of foreign conduct that might violate American laws. He pointed out that “there is no evidence that Congress has ever weighed the costs and benefits of authorizing court orders.”

Id.


59 Id. at 210–16.
Two courts distinguished this reasoning. In *In re Info. Associated with One Yahoo Email Address That Is Stored at Premises Controlled by Yahoo*, the government made an application for a warrant pursuant to 18 U.S.C. § 2703 to compel Yahoo to disclose e-mail records, specifically, "all responsive information—including data stored outside the United States—pertaining to the identified account that is in the possession, custody, or control of Yahoo." Likewise, a second case, *In re Information Assoc. with [Redacted]@gmail.com*, rejected a motion to quash subpoenaed records from Google stored internationally. The court reasoned that Google’s representatives in California could access, compile, and disclose to the government the subject records and information with the push of a button and without ever leaving their desks in the United States.

As previously stated, the issues raised in the *Microsoft* case were ultimately resolved by the CLOUD Act, making electronic information generally accessible to the U.S. government on the basis of public welfare and terrorism. Upon interpretation of this act in civil litigation, potential litigants must consider disclosure obligations when evaluating the terms of a prospective cloud computing agreement. In other words, when considering cloud storage, a customer must be aware of how one can preserve the information in order to be ready for litigation, including multijurisdictional and extraterritorial data storage and transfer.

**B. Strategies for Preserving Information Stored in the Cloud**

Pursuant to FRCP Rule 34(a) a party may request during litigation the production of documents and various other categories of items that are “in the responding party’s possession, custody, or control.” The items that may be sought under the rule include “electronically stored information”—both electronic communications and archived copies of such communications that are preserved in electronic form. Thus, putting aside the multijurisdictional and extraterritorial issues, disclosure responsibilities are complicated by the delegation of “control,” which “complicat[es] the decision a business makes about storing critical or sensitive data in the cloud.”

Regarding what constitutes “control,” the Sixth Circuit and other courts have held that documents are deemed to be within the “control” of a party if the party "has the legal right

62 Id.
63 Cindy Pham, *E-Discovery in the Cloud Era: What’s a Litigant To Do?*, 5 HASTINGS SCI. & TECH. L.J. 139, 180 (2013) (“[An] attorney should work closely with the company’s IT staff to understand what kind of cloud infrastructure the company uses . . . , what is stored in the cloud, what the terms of the service agreement are, and what data retrieval options and tools are available.”).
64 Fed. R. Civ. P. 34(a)(1) (emphasis added); *see also* Cooper Indus., Inc. v. British Aerospace, Inc., 102 F.R.D. 918, 919 (S.D.N.Y. 1984) (“Documents need not be in the possession of a party to be discoverable, they need only be in its custody or control.”).
to obtain the documents on demand." In light of the rule's language, “[a] party responding to a Rule 34 production request ‘cannot furnish only that information within his immediate knowledge or possession; he is under an affirmative duty to seek that information reasonably available to him from his employees, agents, or others subject to his control.’” The requisite “legal right to obtain” documents has been found in contractual provisions that confer a right of access to the requested materials.

For purposes of potential litigation, parties also must consider the retention practices of a given cloud provider. A cloud customer that has decided to engage a cloud provider should do so mindful of its duty to maintain records, regardless of the contract or the service provider's ability to supply the records. Customers should therefore contemplate agreements for the return or transfer of their data. Indeed, electronic evidence in litigation may be treated like any other evidence, and litigants may be penalized for failing to turn over such information. Although it is not expected for a party to save "every shred of paper" upon recognizing litigation, a litigant still has the "duty to preserve what it knows, or reasonably should know, is relevant in the action." In an effort to comply with a duty to preserve evidence, a party will be free to preserve electronic evidence in any format it chooses, including inaccessible formats if those are considered material for discovery.

Finally, as in any litigation involving electronic evidence, data authentication is potentially an issue in cloud computing disputes. As with other cloud computing issues, the core authentication concern for electronic evidence stored in the cloud is the company's loss of direct control over the information. In short, the terms of the cloud computing contract and data management as it relates to the cloud computing service must be consistent with authentication requirements. Although there is no extensive guidance on authentication of cloud-stored information, courts have warned that there is no difference in data authentication requirements as between electronically stored information and information recorded on paper. If anything, one must be aware that electronic data might be held to a higher standard because information can be easily manipulated. Success in authenticating data generally does not depend on “legal or factual arguments, but rather

---

67 In re Bankers Trust Co., 61 F.3d 465, 469 (6th Cir. 1995); see also Mercy Catholic Med. Ctr. v. Thompson, 380 F.3d 142, 160 (3d Cir. 2004); Searock v. Stripling, 736 F.2d 650, 653 (11th Cir. 1984).
70 Pham, supra note 63, at 181–82 (an attorney working with a client who contracted with a cloud provider should attempt to learn “where the data is physically located and what the cloud provider’s archival and retention capabilities are”); see also Hinkes & Gaukroger, supra note 66, at 51.
72 Id. at 103–04; Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 218 (S.D.N.Y. 2003).
73 Steven W. Tepper, Testable Reliability: A Modernized Approach to ESI Admissibility, 12 Ave Maria L. Rev. 213, 217 (2014) (“The inherently mutable nature of computer-generated data creates new issues that have a significant and detrimental effect on reliability, authentication, and ultimately on the issue of admissibility.”); see also Pham, supra note 63, at 160 ("[S]ince the Federal Rules do not require that a third-party cloud provider preserve evidence without a duty to so do, once the information is located, preserving potentially relevant ESI may be difficult, if not impossible.").
74 Griffin v. State, 419 Md. 343, 351 (2011) ("A number of social networking websites, such as MySpace, enable members to create online profiles . . . Anyone can create a MySpace profile at no cost . . .") (citations and quotation marks omitted; emphasis added).
the amount of time and resources a litigant devotes to the problem." Thus, an attorney using cloud services must be mindful of the "basics" of data authentication and its admissibility. Is the information stored relevant to potential litigation? Different authenticating factors will apply to different types of information. A good practice is to be mindful of the usual form of proof when working with a cloud clause to ensure a practitioner or other interested party is not impaired or unable to authenticate data.

IV. Strategies for Mitigating Business Interruption When a Cloud Provider Declares Bankruptcy

When choosing a cloud provider, a customer should consider how its business will be affected if the cloud provider files for bankruptcy protection or, in the worst-case scenario, goes out of business. This is particularly important if the cloud provider will be providing data storage or processing services or access to critical software applications because a customer's business operations could be significantly impaired if it were to lose access to crucial data or software applications.

Cloud providers typically file for bankruptcy protection under either Chapter 7 (liquidation) or Chapter 11 (reorganization) of the Bankruptcy Code. Under Chapter 7, the debtor's nonexempt assets are liquidated, and the proceeds are used to pay the creditors, whereas under Chapter 11, the debtor may elect to either: (1) restructure its financial obligations so that it may emerge from bankruptcy and continue to operate its business under a court-approved plan of reorganization; or (2) liquidate its assets. Whether the bankruptcy petition is filed pursuant to Chapter 7 or Chapter 11, a customer must have a backup plan for the worst-case scenario: that it no longer has access to any data stored in the cloud provider's environment or to critical software applications.

A. The Bankruptcy Estate

Chapter 7 and Chapter 11 bankruptcy cases begin with the filing of a bankruptcy petition with the bankruptcy court by either the debtor or the creditors of the debtor who meet certain requirements. The bankruptcy is considered voluntary if the petition is filed by the debtor and involuntary if filed by the creditors. In both Chapters 7 and 11 cases, the filing of the bankruptcy petition triggers the creation of the bankruptcy estate. The bankruptcy estate consists of all property in which the debtor had an interest at the time of the filing of the petition.

76 Hon. Paul W. Grimm et al., *Authenticating Digital Evidence*, 69 Baylor L. Rev. 1, 11 (2017) ("[T]he importance of any factor will be case-dependent. And there is no intent to imply that all of the factors listed must be met before the proffered digital evidence can be found authentic.").
77 The Federal Rules of Evidence provides that information about a process or system can be authenticated by "describing a process or system and showing that it produces an accurate result." *Fed. R. Evid.* 901(b)(9).
79 *Id.* §§ 1101–1174.
80 *Id.* §§ 101–1532.
In Chapter 7 bankruptcy cases, the bankruptcy estate is administered by a trustee whose primary role is to liquidate the debtor’s assets and distribute the proceeds to the nonsecured creditors. In Chapter 11 bankruptcy cases, unless a trustee is appointed, the debtor becomes the “debtor-in-possession” and remains in control of the bankruptcy estate while the business undergoes reorganization or liquidates its assets.

If a customer’s data is to be stored in the cloud provider’s environment, it is critical that the cloud services contract clearly state that the customer will remain the owner of any confidential or proprietary data provided by the customer to the cloud provider so that the customer’s confidential or proprietary data is not considered part of the bankruptcy estate. In addition, to ensure that any confidential or proprietary data generated by the cloud provider while performing the services is owned by the customer and not the bankruptcy estate, the cloud provider contract should include a present assignment of the cloud provider’s rights in that confidential or proprietary data to the customer.

If the cloud provider contract includes software development services, a customer should also confirm that the cloud provider contract includes a provision assigning ownership to the customer of any software developed by the cloud provider.

B. The Automatic Stay

The filing of the bankruptcy petition under either Chapter 7 or Chapter 11 also triggers the automatic stay (an injunction that prohibits creditors from attempting to collect debts that arose before the filing of the bankruptcy petition). The automatic stay prohibits the commencement or continuation of any action or proceeding against the debtor, including collection activities, foreclosures, repossessions of property, and lawsuits.81

The primary purpose of the automatic stay is to give the debtor a “breathing spell” from creditors so that it can focus on formulating a reorganization plan or liquidate its assets while continuing to operate the business without interference from the creditors. Under Chapter 7, the trustee may be authorized for a limited period of time to operate the business if the operation “is in the best interest of the estate and consistent with the orderly liquidation of the estate.”82 Under Chapter 11, the debtor as the debtor-in-possession may continue to operate the business while it prepares the plan of reorganization.83

Although a business may continue to operate following the filing of the bankruptcy petition under either Chapter 7 or Chapter 11, this does not guarantee that the debtor or trustee, as applicable, will continue to operate the business, even if all actions or proceedings have been stayed. Customers should keep in mind that the debtor may not be in a financial position to continue to operate the business and that the trustee may not have the necessary experience to run the business. A customer should also keep in mind that even if the business continues after the filing of the petition, the period of time during which the debtor or trustee, as applicable, continues to operate the business might not be long enough for the customer to migrate its data and systems to a new cloud provider. To protect itself from this situation, a customer may want to include a provision in the applicable contract requiring the cloud provider to store a backup copy of the data with a third-party provider and perform regular updates to that data.

81 Id. § 362(a). Certain types of actions are excluded from the automatic stay. Id. § 362(b).
82 Id. § 721.
83 Id. §§ 1107–1108.
C. Executory Contracts

One of the benefits of both Chapter 7 and Chapter 11 bankruptcy is that the trustee or debtor-in-possession may, with some exceptions, assume or reject executory contracts to which it is a party. An executory contract is one in which the parties to the contract have material obligations yet to be performed at the time of the filing of the bankruptcy petition. Executory contracts typically include both software license agreements and cloud provider contracts.

If the trustee or debtor-in-possession assumes the executory contract, then it will be required to continue performing its obligations under the contract. For a customer of a cloud provider contract that is assumed, this is good news because the customer will continue to have access to the services provided by the cloud provider under the contract and its data.

On the other hand, if the trustee or debtor-in-possession rejects the executory contract, then it will not be required to perform any of its obligations under the contract. The rejection will be treated as a material breach of the contract by the debtor, and the customer will obtain an unsecured claim for money damages. For a customer, rejection of its cloud provider contract means that it will no longer have access to the services.

The Bankruptcy Code gives licensees of intellectual property certain protections when the trustee or debtor-in-possession rejects its licensing agreement. Under section 365(n) of the Bankruptcy Code, a licensee may elect to retain its rights to the licensed intellectual property (including to any embodiments of the intellectual property, such as the source code of the software and any documentation). If the licensee elects to retain its rights to the licensed intellectual property, it must continue to pay any licensing fees. The licensor will not be required to perform any of its obligations under the contract, however, including any of its maintenance obligations. For the licensee, this means that the licensor will not have to make available any updates, upgrades, or bug fixes to the licensed software. This could be problematic unless the licensee has the necessary resources to maintain the software (such as by modifying the source code or developing additional code) while it looks for another solution to meet its needs.

Whether section 365(n) applies to cloud provider contracts will depend on whether the bankruptcy court decides that the trustee or debtor-in-possession is a licensor of a right to intellectual property. Given that cloud vendor agreements do not typically include grants of copyright licenses because the customer is not receiving a copy of the software, it is not clear whether the bankruptcy court will find that section 365(n) applies to the cloud provider agreement. Although not binding on the bankruptcy court, customers could increase the likelihood that the bankruptcy court will find that section 365(n) applies to their contract if the cloud provider agreement is drafted so that it conforms to the language and the requirements of section 365(n) (i.e., drafting the cloud provider contract as a license to intellectual property). The addition of such language will depend on the type of services provided by the cloud provider (e.g., SaaS, PaaS, or IaaS) because, in some instances, such license grant will not be consistent with the rights granted to the customer.

86 Id. § 365(n)(2)(C)(ii).
If the bankruptcy court finds that section 365(n) applies, the customer will have the right to elect to continue to use any software applications that are hosted by the cloud provider and to obtain a copy of the object code, source code, and documentation.87 However, because the cloud provider will not be required to continue to host the software application or meet any of its service-level commitments, the customer must either host the software internally or find a third-party vendor to host the applications and provide the service levels.88 This may give the customer a temporary solution while it identifies an alternative solution.

D. Strategies for Mitigating Business Interruption

What can the customer do to prevent business interruption if its cloud provider files for bankruptcy protection, or worse, goes out of business?

If the cloud provider’s services are critical to the operation of the business, then the customer should probably prepare for the worst. The customer should focus on developing a reliable, practical, and cost-effective solution that will allow the customer to continue to access the services and its data in the event its cloud provider goes out of business. This may include developing a short-term solution that will allow the customer to continue having access to the hosted software applications and its data while it identifies an alternative solution to meet its business requirements.

Depending on the importance of the data to the customer, the customer may want to include provisions in the cloud provider agreement requiring the cloud provider to store a backup copy of the data with a third-party provider and perform regular updates to that data. If the customer has the resources to bring the data in-house, the customer may include provisions in the cloud services agreement requiring the cloud vendor to deliver periodic copies of all data to the customer. In either case, the cloud provider should be required to deliver the data in the right format so that it can be easily accessed and used by the customer and any third-party provider.

If the hosted software applications are critical to the operation of the business, and the customer has the necessary resources to deploy the software application in-house, the customer should consider setting up a third-party escrow agreement with a third-party agent. Pursuant to the escrow agreement, the cloud provider would be required to place the source code of the software application, relevant documentation (including user manuals), and a list of any third-party software necessary to run the software into escrow. The cloud provider would also be required to provide periodic updates to the escrowed materials to ensure that escrowed materials reflect the latest versions of each of the escrowed materials. The escrowed materials would be released to the customer upon the filing of the bankruptcy petition. The cloud provider contract should also include a present license to use the source code and documentation, effective as of the release of the escrowed materials. The license grant should be drafted as a present grant (including the language “hereby grants”) so that the customer may rely on section 365(n) in the event the cloud provider rejects the cloud vendor contract.

Choosing a cloud provider is an important decision, particularly if the cloud provider will be storing the customer’s data or hosting mission-critical applications. A customer

87 *Id.* § 365(n)(4)(A)(ii).
88 Part IV.D, below, suggests a strategy for accomplishing this.
must be proactive in implementing a backup plan that will allow it mitigate the negative
effects to its business if its cloud provider goes out of business.

V. Conclusion

Alternative Dispute Resolution (“ADR”) is the use of processes or methods for deci-
sion-making, such as mediation and arbitration, to resolve a dispute instead of litigation.

As supported by a study by the WIPO Center, the benefits of including ADR clauses in
cloud-computing agreements include time and cost savings. ADR clauses also help main-
tain confidentiality as to proprietary data and the ultimate outcome of a case, as well as
minimize business disruption. Indeed, dispute-resolution procedures may be tailored to,
among other things, the specific circumstances of the technology, the confidential or pro-
prietary nature of the subject data, and the unique dynamics of the business relationship.

A well-written ADR clause can also help an entity avoid the uncertainties of evolving
legislation, such as the CLOUD Act and the SCA, and the ongoing interpretation of same.
New legislation, however well-intended, remains relatively open to interpretation. This
leaves one's personal and sensitive information potentially unprotected. Moreover, for
purposes of potential litigation, parties also must consider the retention practices of a
given cloud provider, the authentication of data, as well as the return or transfer of data.

In sum, considering the many benefits of ADR clauses as noted above, cloud comput-
ing agreements should contain express ADR language.