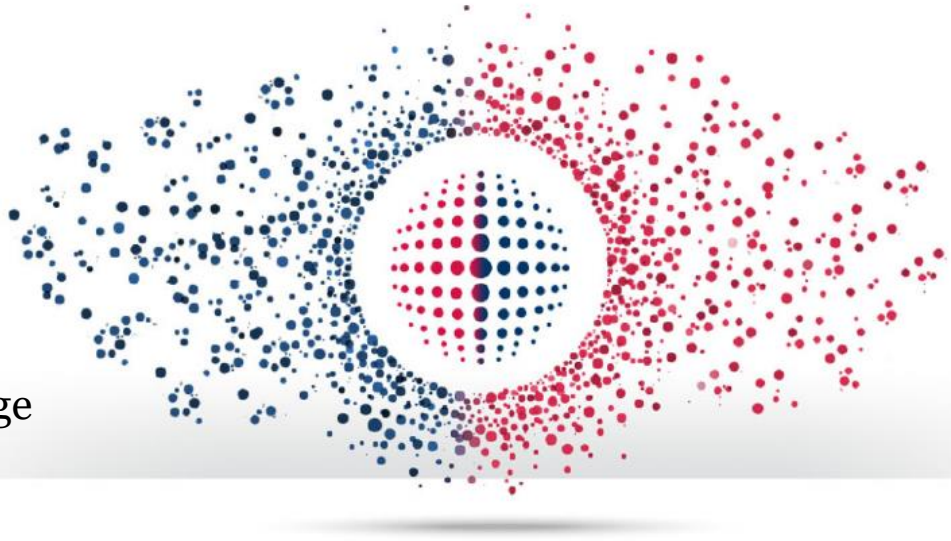
CPR
International Institute for
Conflict Prevention & Resolution



Mediation of Cyber Disputes: ADR Moves into the Digital Age

By Kenneth N. Rashbaum

As originally appeared in ***Law360***

BYLINED ARTICLE | JULY 2017

Over ninety-five percent of all business information is in digital format, and that paradigm presents a host of potential dispute issues. Electronic information is just fundamentally different from paper information: There is more of it (how easy is it to tap out a text?); it is in many places at the same time; it's easier to lose or alter. And it's protected by myriad regulations and laws, in the U.S. and elsewhere in this globally-connected economy. Digital information, then, is a breeding ground for disputes. Fortunately, this dispute minefield need not blow up the organization's budget. Mediation provides an exemplary way to control dispute costs, and more and more contract drafters are including some form of alternative dispute resolution in their agreements.

Relatively few cyber disputes arise from government regulatory proceedings or litigation. Most conflicts that arise from breaches of information have their roots in agreements between the parties as to how that information would be maintained. Attorneys who prepare service level agreements, end user license agreements for applications and other software, contracts regarding sales and service of interconnected devices (i.e., fitness and health tracking devices and connected medical devices such as pacemakers and defibrillators) or other agreements that comprise the uses and management of electronic information often include metrics for information management. These standards, by which one party will maintain electronic information in compliance with legal standards, such as the HIPAA Security Rule, SEC Regulation S-P Section 30, or privacy and security laws of state such as Massachusetts, California or New York, or industry metrics like ISO (International Standards Organization) 27001. Following a breach, an aggrieved party may contend that these standards were not met. These can be particularly contentious disputes requiring significant costs for forensic analysis and expert testimony.

> "'Most conflicts that arise from breaches of information have their roots in agreements between the parties as to how that information would be maintained."

Contract drafters know that every agreement is a dispute waiting to happen, and so frequently include alterative dispute

provisions to mitigate the costs when the inevitable occurs. This is particularly so when the subject matter involves a new and rapidly changing areas of law such as privacy, confidentiality and cybersecurity. Drafters take great pains to prepare clauses that purport to limit liability disclaim warranties and shift liability through indemnification, but do these clauses actually accomplish their intended goals? Disclaimers warranty limitations may withstand court challenges, but at what cost in terms of legal fees and damaged reputation when the disputes find their way to social and mainstream media?

Transactional lawyers and litigators may put faith in indemnification provisions that purportedly can shift costs in the event of data breaches or regulatory proceedings, but this reliance is often misplaced. Many states construe indemnification provisions strictly against the draft, so an indemnification demand pursuant to the contract may not survive a challenge to the clause. The trigger for indemnification is often "intentional misconduct, "gross negligence," or "violation of the terms of this agreement." These are most often questions of fact, which rarely can be resolved by dispositive motion practice and, instead, require tens or hundreds of thousands of dollars in discovery and trial costs. Cost shifting through indemnification clauses, then, may turn out to be a very expensive effort that amounts to tilting at windmills.

Do clauses that require the parties to carry cyber risk insurance requiring one or both parties to name the other as an additional insured offer respite from the litigation morass? Not really. Cyber risk is a young insurance line. Carriers differ widely in their policy language, and case law is not consistent between circuits and districts in the interpretation of certain coverage provisions. Definitions of covered "wrongful acts" may not be worded with the precision lawyers would like to see, as is the case with certain exclusions such as those that apply to intentional misconduct, regulatory coverage (in some policies), and certain often ill-defined security incidents.

"Cyber risk is a young insurance line. Carriers differ widely in their policy language, and case law is not consistent between circuits and districts...."

Other gnarly insurance issues may include sub-limits for certain coverages, self-insured retention amounts, retroactive dates (significant, as malware may be in the systems well before the effective date of the policy) and timely reporting of incidents where, indeed, the malware or social engineering attack (i.e., malware embedded in seemingly-innocent emails or a directed email requiring a money transfer to the hackers) may be discovered after the date that the policy requires the incident to be reported. Because of the complexity and potential costs of cyber insurance coverage disputes, insurers and many insureds have looked to mediation as a way to contain cost as this area of law matures.

For reasons of financial savings, efficiency and plain peace of mind, those who prepare agreements in technology areas have increasingly turned to mediation and other dispute resolution clauses and this, in turn, has created a demand for mediators with backgrounds that comprise multiple practice areas, including cybersecurity, privacy, technology transactions and litigation. And they should open to dispute-mitigation alternatives. For example, arbitration clauses

have been around for a very long time but newer and possibly less expensive modalities include "cooling-off and mediation" provisions that require the aggrieved party to notify her counterpart of the disputed matter and then, only after a certain period of time, the parties will proceed to mediation and can only go further, to arbitration or litigation, if mediation fails.

"For reasons of financial savings, efficiency and plain piece of mind, those who prepare agreements in technology areas have increasingly turned to mediation and other dispute resolution clauses and this, in turn, has created a demand for mediators with backgrounds that comprise multiple practice areas, including cybersecurity, privacy, technology transactions and litigation."

Cybersecurity, privacy and confidentiality, cyber risk insurance and technology contract law are among the most dramatically shifting areas of the legal landscape. Rather than spending hundreds of thousands of dollars to try to fashion the law to a party's favor, with the risk of creating bad law, cooler heads are prevailing and, as a result, the demand for cyber mediation has increased and will continue to grow. The laws of legal economics will abide no other result.

—By Kenneth N. Rashbaum, Barton LLP

Kenneth N. Rashbaum
Barton LLP

Kenneth N. Rashbaum, Esq. is a Partner at Barton LLP and a Distinguished Neutral on The CPR Institute's new Cyber Panel.

ABOUT CPR

CPR is the only independent nonprofit organization whose mission is to help global business and their lawyers resolve commercial disputes more cost effectively and efficiently. For over 30 years, the legal community has trusted CPR to deliver superior arbitrators and mediators and innovative solutions to business conflict.

CPR
30 E 33rd Street, 6th Floor
New York, New York 10016
Phone: +1.212.949.6490
Fax: +1.212.949.8859
www.cpradr.org