

# Chicago Daily Law Bulletin®

VOLUME 165, NO. 234

LAW BULLETIN MEDIA.

SPONSORED CONTENT

## The Benefits of ADR in the Cyber Context

By STEVEN GILFORD, ESQ.

For a number of years, I have been the lead author of “Insurance Coverage for Data Breaches and Unauthorized Privacy Disclosures,” a chapter in the Practising Law Institute’s well-regarded publication *Proskauer on Privacy*. We update the chapter each year in an effort to keep it as current and comprehensive as possible.

This year, as I worked on the annual update, I was struck by the appropriateness of mediation and, if necessary, arbitration for resolving coverage and other disputes concerning cyber issues. The cyber space constantly presents new issues. Consider two recent examples.

The first example involves insurance exclusions for government-sponsored activity and for war or warlike action. These kinds of exclusions present complex issues in today’s world, where hacking into government or corporate servers is often alleged to be the handiwork of foreign governments of countries like China, Russia or North Korea. The recent decision by the Ninth Circuit Court of Appeals in *Universal Cable Productions, LLC v. Atlantic Specialty Insurance Co.*, 929 F.3d 1143 (9th Cir. 2019) involved a situation in which Universal believed it could no longer

guarantee the safety of the Jerusalem production set for its TV series *Dig* after Hamas fired rockets into Israel and engaged in a number of other hostile activities. When Universal submitted a claim under a television production insurance policy, the insurer denied coverage, relying on a policy exclusion of expenses resulting from “war,” “warlike action by a military force,” or “insurrection, rebellion, or revolution” (*Id.* at 1147). Having concluded that “the insurance industry has a customary usage that limits exclusions for ‘war’ to hostilities between de jure or de facto sovereigns” (*Id.* at 1157), the court devoted a substantial number of pages in its opinion to analyzing the role of Hamas in the Middle East in an effort to determine whether it was a sovereign for purposes of the asserted exclusion (*Id.* at 1147-48, 1157-59, 1160-61). The history of Hamas and Israel is well known. But this is not always the case in the cyber world. It is hard to imagine, for example, the complexities of trying to determine whether an unknown cyber criminal in Russia or North Korea was government sponsored or directed, particularly if courtroom evidentiary procedures are applied.

Another recent example involved a coverage dispute



Steven Gilford

concerning cryptocurrency. The one case that seems to have addressed the issue in an insurance context is the brief 2018 trial order of the Ohio trial court in *Kimmelman v. Wayne Insurance Group*, 18 CV 041 (Court of Common Pleas, Franklin County, Ohio, Sept. 25, 2018). In that case, Kimmelman submitted a claim under his homeowner’s insurance for stolen bitcoins, which he claimed were worth \$16,000. The insurer investigated the claim and paid Kimmelman \$200, which was the policy sublimit applicable to a loss of “money.” When Kimmelman filed suit, the insurer moved to dismiss, relying primarily on articles from CNN, CNET and the *New York Times* that apparently referred to bitcoins as money, as well as on an IRS document that characterized “BitCoin and other electronic property” as “virtual currency” for federal tax purposes (*Id.* at \*1- \*2,

citing IRS Notice 2014-21). Noting that there was no applicable legal authority except the IRS notice, the court found that bitcoins were not “currency,” because they are not recognized by the United States, but that they were “property” because the IRS had taken the position that “for federal tax purposes, virtual currency is treated as property” (*Id.* at \*2, quoting IRS Notice 2014-21). Kimmelman involved a relatively small claim, so it is likely that limited resources were available to litigate the issue, but the question of whether bitcoins are currency can be the subject of extensive economic and expert analysis.



In addition to issues of what was stolen, cryptocurrency presents complex issues of valuation. The value of cryptocurrency can vary widely. For example, the value of a bitcoin ranged from \$6,589 on January 1, 2018; to \$3,742 on December 31, 2018; to \$118,011 on June 24, 2019 and \$7,146 on November 25, 2019. Valuation of other, less-well-known cryptocurrencies can

vary even more dramatically. Property policies typically look to actual cash value or replacement cost as a basis for loss adjustment, but what happens where the value is \$3,000 on the date of the theft, \$12,000 on the date of discovery, \$8,000 on the date a proof of loss is submitted and \$20,000 when the claim is paid? These are issues that have not been considered, much less resolved, by the courts.

Given the novelty and complexity of these issues, mediation and arbitration provide attractive alternative dispute resolution (ADR) mechanisms for disputes in these areas, particularly where insurance coverage is involved. Initially, both arbitrations and mediations have the advantage of not normally being constrained by strict rules of evidence. This allows the use of experts, literature and information that may not be strictly admissible in

a traditional courtroom setting. It also can help to avoid the costs of extensive discovery (and the complexity and obstacles often inherent in international discovery), which may be needed to obtain evidence admissible in a court proceeding.

Another advantage is that both arbitration and mediation are typically confidential and thus not precedential, so the parties can resolve their differences without necessarily creating precedent that will control the resolution of similar issues among themselves or with other parties. This can permit a more businesslike resolution informed by the history, goals and objectives of the parties as opposed to strict legal principles that were not necessarily designed for today's world of cyber and digital technology. Moreover, mediations and arbitrations can make use of arbitrators and mediators

who are knowledgeable in relevant industry practices and the kinds of technical issues involved in the cyber space. Where insurance is involved, technical expertise of a mediator or arbitrator can help integrate traditional insurance concepts with rapidly changing insurance products and the facts of a cyber dispute.

Arbitration and mediation generally require agreement of the parties. Often arbitration, and sometimes mediation, is required by an applicable cyber agreement or insurance policy. Even if it is not, parties can agree to the use of ADR procedures. In the case of mediation, the parties can agree to mediate even when a dispute is otherwise before the court. Mediation and settlement can be particularly useful in situations where both parties have strong positions but do not want to risk an all-or-nothing result in a judicial forum. Ultimately, while

mediation can facilitate the exchange of information in a confidential setting and can allow parties to try to find a way to resolve their differences, the process remains in the control of the parties, which must agree upon mutually acceptable terms in order to reach a settlement.

Given the uniqueness of the issues and the potential proof difficulties, mediation and arbitration should be carefully considered as means of resolution of complex cyber disputes. Ideally, these procedures can be built into the contracts that govern the parties' relationships. Even when that is not the case, ADR mechanisms can be agreed upon by parties as a more effective and efficient mechanism for resolving their disputes.

*Steven Gilford, Esq., is mediator and arbitrator at JAMS. He can be reached at [sgilford@jamsadr.com](mailto:sgilford@jamsadr.com).*