When COVID-19 Era Software Disputes Become Nuclear Litigation Events

By Kamal Ghali and Christopher T. Giovinazzo

Even before COVID-19 transformed thousands of companies into remote work workforces, software meltdowns have always risked catastrophic consequences for any business. Virtually every major company, from consumer product makers to business-to-business service providers, powers its business with complex and expensive software. And even before the economic havoc wrought by COVID-19, companies across the country—in scores of different sectors including finance, technology, aviation, and healthcare—have been embroiled in high-stakes lawsuits about the software their businesses depend on. These lawsuits—brought by private actors and governmental agencies—have similarities, namely, hotly disputed allegations about how the software works, and eye-popping claims about the damage caused by faulty software. As businesses now layer in new sets of software to securely facilitate remote work, and as company budgets are stretched by the economic shocks of the pandemic, the consequences of such technology meltdowns may be even higher.

Software litigation disputes tend to fall into a familiar pattern. Disgruntled software buyers often seek damages well beyond the already large software sticker-price. And they often include allegations that the faulty software crippled a plaintiff's business operations. Just last year, Hertz, the rental company, sued Accenture after Hertz spent $32 million dollars for Accenture to develop an e-commerce platform and apps to "transform the digital identity" of Hertz's rental car business. Hertz says the software failed, and it wants its money back and more. Likewise, the city of Jackson, Mississippi recently sued Siemens contending that faulty software failed to accurately measure how much water Jackson citizens consumed, causing nearly half a billion dollars in damages.

More and more frequently, commercial software suits also claim that alleged security vulnerabilities in the software financially harmed the plaintiffs. Take, for example, the recent avalanche of allegations against Zoom Video Communications, Inc., arising out of security vulnerabilities in its software and its allegedly improper disclosure of consumer data. Or take a recent suit by a Pennsylvania credit union against Fiserv for "allegedly failing to address persistent vulnerabilities in the platform that powers its banking websites and online applications." The lawsuit contends, among other things, that security vulnerabilities in Fiserv's software are "wreaking havoc" on the credit union's customers. Likewise, Cisco Systems recently settled a False Claims Act case accusing Cisco of selling video surveillance software riddled with security vulnerabilities.

Other suits accuse companies of deploying software for deliberately nefarious reasons. An Israeli court recently rejected a motion to dismiss filed by NSO Group, in a case where a "prominent Saudi activist" claimed that NSO's "cyberweapons were used to hack his phone." Similarly, WhatsApp recently filed suit against NSO in federal court in California alleging that the company's "spy technology" was deployed on WhatsApp users. Even apart from cases of

purported international espionage, some plaintiffs are claiming that software was intentionally fraudulent, as claimed in a putative class of Tesla owners who say Tesla's software update fraudulently limited the car's "battery range."

While some of these disputes, especially those involving spy technology, may be difficult to plan for, there are certain things companies can do to limit the risks and fallout from disputes over the creation, use, and deployment of software, especially as they increase the scale of their remote business operations.

First, document any major software agreement—not just initially—but throughout implementation and use. Multi-year contracts for sophisticated software generally fail to anticipate the ways in which the parties' goals and expected software functionality can change as development is underway. And too often, buyers don't have a clear understanding of what they want (or exactly how the software will work) until the project is well under way. Companies that document changes to the scope of work (and appropriately track the project's evolution), can avoid miscommunication and be better positioned should a dispute escalate into full-blown litigation.

Second, protect your proprietary information. These days, contracts for customized, complex software can often require giving third parties significant remote access to sensitive—and proprietary—information. Ensuring that the contract clearly spells out restrictions on the access to certain data, non-disclosure obligations, methods to get the data back after the contract ends, and clauses on who owns the data, can prevent serious problems should the relationship sour.

Third, companies contracting for software should think carefully about whether the contract language provides an adequate remedy should the software malfunction or fail to properly launch. Most software looks great during the sales presentation; but too many software problems only surface during or after deployment, at which point the company may be crippled if the software shuts down. The best software contracts carefully allocate risk and address what happens (and who pays for it) if the software malfunctions or suffers from security vulnerabilities discovered after the project ends.

Lastly, when a dispute heats up or where litigation is unavoidable, companies should work with outside counsel experienced in explaining highly technical concepts to judges, juries, or arbitrators. Success in major software disputes, as well as any complex business dispute, depends on clear and concise advocacy, and not the technical jargon and unhelpful detail that too often accompanies software disputes. Moreover, working with experienced outside counsel may help facilitate a quick settlement and business solution before one side preemptively files a lawsuit that may only complicate efforts to negotiate a resolution.

Companies are now grappling with the economic fallout of COVID-19 and embracing what may be a new era of increased reliance on remote work and new software agreements to facilitate business. Part of navigating this new environment will require companies to take stock of what types of software their businesses depend on and developing plans for how to overcome and quickly resolve disputes that risk significantly disrupting business operations.

Kamal Ghali is an experienced trial lawyer and a former U.S. Department of Justice white-collar and cybercrime prosecutor. He leads the cyber & digital litigation practice at Bondurant, Mixson & Elmore. He can be reached at ghali@bmelaw.com.

Christopher T. Giovinazzo has served as lead trial and appellate counsel in software contract disputes, including a recent federal jury trial in which his client obtained a multi-million dollar verdict. He is a partner at Bondurant, Mixson & Elmore and serves as the General Counsel. He can be reached at giovinazzo@bmelaw.com.

A previous version of this article appeared on Law.com on Feb. 4, 2020.