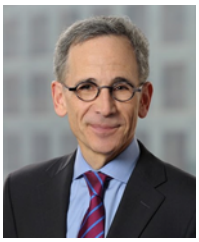
Bloomberg Law®

bloombergbna.com

INSIGHT: Cybercrime & Sports–The Law of Unintended Consequences



By Craig A. Newman

Justice Samuel A. Alito Jr.—the U.S. Supreme Court's foremost baseball fan—wrote the majority opinion in a decision striking down a 1992 federal law that effectively banned commercial sports betting in the United States. It's doubtful he intended to hand cybercriminals a major—and highly lucrative—judicial victory, but he may have.

The court's 6-3 ruling in *Murphy v. National Collegiate Athletic Association* invalidated the Professional and Amateur Sports Protection Act, which forbade states from allowing sports gambling. Congress passed the law in the early 1990s to protect the integrity of the game and only allowed one state, Nevada, to offer legalized sports betting.

Yet the decision itself—based on a routine constitutional issue that focused on states' rights—has cleared the way for states to pass laws that legalize collegiate and professional sports gambling.

States Begin to Legalize Sports Gambling Eight states, including New Jersey, Pennsylvania, and Rhode Island, have already done so, and nearly three dozen states aren't far behind. New York, too, is moving toward legalized sports betting. In January, the State Gaming Commission published a set of proposed rules that would permit in-person sports betting at four of the state's upstate casinos.

At a public hearing in January, the commission made clear that ''[t]he proposed [r]egulations seek to protect the integrity of wagering and underlying contests. . . .'' The rules are now subject to a 60-day public comment period. If the proposed rules pass muster, sports wagering could become reality this summer. But for New Yorkers, online betting—an even more lucrative slice of the sports gaming pie—isn't in the cards, at least now.

It didn't take long for casino owners, sports teams and their ownership to embrace the Supreme Court's ruling and the new opportunities it might present. Ted Leonsis, owner of the NBA's Washington Wizards and NHL's Washington Capitals, said in a statement that ''[t]his is a new frontier for professional sports.'' And in a blog post he noted that betting is a natural outgrowth of ''data analytics.''

''The appetite for sports betting is there, and now, instead of offshore bookmakers reaping the benefits, we have a pathway to bring this revenue into the U.S. economy,'' Leonsis wrote. He got it half right.

Hackers Follow the Money Cybercriminals follow the money. And in sports gaming—legalized or not—there's plenty of it. Sports gambling is big business. Although reliable information on size of the illegal sports betting market is hard to come by, it's estimated to be at least $150 billion and as much as $400 billion each year in the U.S. alone.

And the legitimate sports gambling market is off to a fast start. Sports gambling has been legal in New Jersey since June 2018, and in the final six months of the year, New Jersey generated more than $1.2 billion in wagers, with nearly two-thirds from online betting. That's according to the state's Division of Gaming Enforcement.

With so much money at stake, everyone will be looking for ways to cash in, but it's the hackers who are likely to come out on top.

Let's start with the sheer value of sports data. Its early value was popularized in Michael Lewis's book, ''Moneyball,'' which told the story of the Oakland Athletics baseball team and its quest to build a competitive team on a budget.

The general manager, Billy Beane, used statistics to find inefficiencies in the way other baseball teams valued players. By exploiting these statistical anomalies, the A's made the playoffs for two years in a row and teams began to recognize the fact that sophisticated analytics would often mean a competitive edge.

And then there's the fact that sports teams generate mounds of competitive data ranging from scouting reports, the status of contract negotiations, potential player trades, to injury and health-care information. Plus, there's plenty of other data generated that we don't even know about.

Perfect Storm If hackers are able to access this information, it gives them a highly sought-after competitive advantage. Using purloined data, hackers can place their bets within the guidelines of a completely legitimate and government-sanctioned gambling structure.

With legalized gaming, there are rules and regulations that must be followed, licenses to be issued and taxes assessed and paid. But behind this completely legitimate structure is the opportunity for cybercriminals.

The legalized structure is the perfect storm for a hacker. By using stolen information, the hacker avails him or herself of a completely legitimate system to capitalize on that information. In this way, their activities very much resemble stock market insider trading. And it's an opportunity that comes in so many forms that it's almost like playing a multi-dimensional chess game.

Sports teams themselves have been caught up in hacking scandals. In the U.S., perhaps the most notorious example dates to 2015 when the St. Louis Cardinals' scouting director hacked into the database of the Houston Astros and mined competitive intelligence for more than two years before being caught. For his part, the scouting director was sentenced to nearly four years in prison for corporate espionage.

With legalized sports betting in its infancy, it's not difficult to imagine the ways cybercriminals can take advantage of the new environment.

Straight to a Team's Database There's the most obvious—which is a variation of the Astros-Cardinals exploit—hacking straight into a team's database to steal game day and strategic information. If a hacker knows what's in store for an upcoming game, it's not going to take too much to exploit that information, whether it's an injury report or series of new plays. It's like getting a team's playbook ahead of time.

And there's the less obvious cybercrimes. Hacking into the personal information of players or leagues to gather general intelligence and competitive information. How can such data be used? For example, if a cybercriminal knows that a football team's star quarterback may be facing a four-game suspension, it doesn't take much to construct a bet to leverage that information before the news becomes publicly available and the betting lines change.

At best, we are in the first inning of a very long cat-and-mouse game. As more and more states legalize gambling, hackers will be given more and more opportunities—some of which we cannot even fathom now.

So, what's a sports team or league to do to guard against the hackers? Drop back and reassess the protection of their most precious information. Unlike more mundane data, sports teams should protect their most important information using all available resources. Anything short of that is an open invitation for the hacker community.

Author Information *Craig A. Newman is a litigation partner at Patterson Belknap Webb & Tyler LLP in New York and chairs the firm's Privacy & Data Security group.*