CARLTON FIELDS

Fortnite Suit Highlights Game Cos.' Need For Privacy Vigilance

August 27, 2019

There is no denying the explosive growth and popularity that esports and competitive online gaming have experienced recently. Industry events are grabbing headlines like never before, such as the Fortnite World Cup, where a previously unknown 16-year-old competitor recently won the top prize of $3 million. With the heightened interest and attention, however, comes increased risk of data breaches and similar incidents, along with scrutiny from litigants and regulators alike.

Indeed, game companies are just as susceptible to lawsuits and regulation related to data privacy and cybersecurity as companies in any other industry - if not more so, given the sensitive data they increasingly collect and use.

A recent data privacy class action filed in federal court in North Carolina against Epic Games, the company behind the game Fortnite, serves as a stern warning that game companies must be vigilant when it comes to the collection, use and protection of their users' data. Such vigilance includes ensuring that their privacy programs and incident response guides remain up to date and reflect the unique challenges of this growing industry.

Modern Video Games Collect Troves of Personal Data

Gone are the days of Atari and the original Nintendo Entertainment System, which had no internet connection and did not collect data in any meaningful way. Virtually all modern video games require personal information in order to function. Often, personal information is required just to set up a user account and verify the age of minors in order to purchase and use games.

And the games themselves can - and often do - capture every single action, decision and communication players make, whether players know it or not. This data is used to analyze how players access certain in-game content, which helps game companies determine how and whether to develop the game going forward.

With the advent of new technologies, game data increasingly includes a player's physical characteristics (including facial features, body movements and voice data), surroundings, biometrics and information gleaned from social networks. Indeed, in order for some games to function at all, such as Niantic Inc.'s Pokémon Go and Harry Potter: Wizards Unite, geolocation data is essential. Other games, particularly those that include consequential in-game selections and choices, collect information that may reveal intimate details about the player that bear on key personality traits, such as temperament, fears and even leadership skills.

For the most part, this game data is used responsibly to improve the game experience and enable functionality that players demand. In some instances, however, the data is being used for less altruistic purposes, like figuring out how to maximize monetization, including through use of various forms of microtransactions such as loot boxes, which have received increased regulatory scrutiny of late. Other nefarious examples exist, such as the revelation that the National Security Agency used the mobile game Angry Birds to collect phone numbers, emails and device codes for purposes of mass surveillance.

Regardless of the use, the mere collection and storage of this personal data exposes game companies to newfound liability, including the risk of cyberattacks. And that risk naturally increases the more data the game collects and the longer the data is stored.

Cyberattacks Targeting Game Companies and Associated Legal Exposure

Cyberattacks take many forms and threaten organizations differently depending on the context of the particular industry target. Particularly damaging to the game industry are viruses and malicious code that can cripple systems, distributed denial-of-service attacks that take entire services offline and data breaches that result in the exposure of unencrypted data to unauthorized third parties.

The recent Fortnite lawsuit stems from phishing, which is another form of attack that preys on companies across industries, but that is particularly pernicious when involving game companies. Phishing is a form of social engineering whereby the hacker uses low-tech or nontechnical approaches to cause an individual to compromise security procedures and disclose sensitive information, most commonly through email. To fall victim to this kind of attack requires the user to click on a specially crafted phishing link or attachment designed to look like it came from a legitimate source.

In this instance, that source was Epic Games. To entice users to click on a suspicious link, hackers commonly use the promise of free game credits or steep discounts on in-game currency or items. Once the link is clicked, the hacker is able to steal the user's access token to the game through a malicious redirect and perform an account takeover. Once inside the account, the hacker is able to

control the account and then, where the account is linked to a credit or debit card, make in-game purchases and pose as the player to others online.

Although the phishing vulnerability in this case was patched in December 2018, a class composed of the game's users filed a class action against the company. The lawsuit alleges that the class suffered losses in the form of stolen credit or debit card information linked to their accounts. It also alleges that the hackers used the linked credit or debit cards to purchase in-game currency to boost the stats of the stolen accounts, some of which were sold on the black market. The lawsuit ultimately demands $100 million and, regardless of how it turns out, Epic will incur significant attorney fees and other costs.

The Unique Challenges of a Changing Regulatory Landscape

While the result of this lawsuit is to be determined, the passage of data privacy regulations such as the European Union's General Data Protection Regulation and the California Consumer Privacy Act of 2018 are already making an impact and require even greater diligence on the part of game companies with respect to the data they collect, use and store.

For instance, these new regulatory frameworks are trending toward expanding the definition of "personal data" (or "personal information") beyond mere "personally identifiable information" defined in U.S. state data breach notice laws. Now, "personal data" includes any data elements that relate, either by themselves or along with other data, to an identified or identifiable individual or household. This can have massive implications for a game company that has accumulated, and still retains, vast amounts of personal data on its players - data that was once unregulated.

Moreover, the GDPR and the CCPA impose upon companies various standards of data minimization and transparency previously unseen in the game industry. Under these laws and others being proposed, most game companies must provide users with access to the personal data that is collected and used, and in many instances users must also be afforded the right to opt out of automated processing and profiling. This demands that game companies reassess their data processing practices to determine the extent to which they are engaged in such conduct.

The CCPA, in particular, affords California consumers a new right to object to the "sale" of their personal data to third parties, and the word "sale" is broadly defined to mean the transfer of information for any value, even nonmonetary value.[1]

In addition, these new data privacy laws are expected to lead to an increase in data breach class actions. The CCPA, in particular, gives plaintiffs the ability to sue in a class for breaches in certain circumstances. And because the law permits statutory damages ranging from $100 to $750 per incident per consumer, the plaintiffs may not need to prove actual damages. Consequently, it is not

surprising that 66% of companies are concerned about their future class action exposure as a result of the CCPA.[2]

Recommendations

Businesses and other organizations need to institute meaningful cybersecurity and privacy compliance programs that minimize risk. For game companies, these steps include the following:

- Ensure that the business has in place an incident response guide that is tailored to that company and its industry. This may include provisions for a response in the event the cybersecurity attack compromises online accounts, such as a plan and procedure for dealing with suspicious or fraudulent charges related to user accounts that may have been breached. A comprehensive incident response guide will help the organization detect and respond to a potential incident before it becomes a breach, as defined in the law. And if there is litigation, the presence of an incident response guide will be among the features that can be used to demonstrate the organization's "reasonable security procedures and practices."
- Update all data privacy and information security policies, procedures and programs. Be mindful that statements included in a privacy policy will be scrutinized and, in some cases, used against the company. For instance, the Fortnite lawsuit quotes from Epic Games' online privacy notice and alleges that users relied on the statements concerning how personal information is protected to their detriment. That is why it is often recommended to include disclaimers and avoid superfluous language and promises, particularly those concerning the security of the personal information. In short, only make promises that the company can keep, and then aggressively live up to them.
- Understand what personal data is being collected and how it is being used through data mapping. Data mapping is essentially a process of recording the life cycle of personal data as it is collected, used, stored and shared by the business. This process is essential for an organization to be able to act on a consumer's request related to his or her personal information under laws like the GDPR and the CCPA, and it can be a challenge for game companies that collect a lot of personal data. This is not just a one-time event. A business that has previously engaged in data mapping for the GDPR should leverage that work for new laws, like the CCPA. Given the breadth of the definitions of "personal information" and "selling" under the CCPA, a business engaged in data mapping for the CCPA should consider whether to supplement previous data mapping that may not have incorporated these concepts. And some organizations may find themselves data mapping for the first time.

- Be mindful of data collected and used belonging to minors. Most game companies are already familiar with laws that regulate the collection and use of minors' data, such as the Children's Online Privacy Protection Act, and have policies and procedures in place for complying with them. But with the passage of the CCPA, game companies must once again revisit their policies, in particular for purposes of obtaining the requisite consent for collecting and using such data. The relevant age for purposes of triggering the CCPA's new obligations is 15 and under, whereas the relevant age under COPPA is 12 and under.

Conclusion

This is an exciting time for the esports and electronic gaming industry. But the industry's newfound attention and success brings with it a variety of unique, and unresolved, challenges. Those challenges include significant risks stemming from data collection and the security of that data. The industry players who stand the test of time will be those who are able to develop and maintain games while striving to protect the privacy of their users and the security of those users' data.

[1] Cal. Civ. Code § 1798.140(t)(1).

[2] 2019 Carlton Fields Class Action Survey, available at https://classactionsurvey.com/.

Reprinted with permission of Law360. View original publication here.

Related Practices

Cybersecurity and Privacy
Esports and Electronic Gaming
Litigation and Trials