eSports and US Data Privacy: A Game Worth Winning

November 24, 2020

The business of competitive video gaming, otherwise known as eSports, is booming. Each year millions of gamers and viewers tune in to watch players compete in real-time while they engage with the platform, make in-game purchases, and exchange data through chat functions. It's a billion dollar industry where growth and data are king.

With this growth comes risk. In the United States (US), the eSports industry faces a particularly complicated, and often overlapping patchwork of data privacy and information security laws as it relates to the personal information collected through the use of various platforms. This legal landscape can, and often does present a unique set of compliance challenges for companies looking to operate at the speed of a click, especially as it relates to the collection, use, and transfer of minor children data. Any slip-up can result in significant financial and reputational fallout.

At the federal level in the US, there are two laws that play a particular role in regulating how eSports organizations collect, use, and share the data of its users - the Children's Online Privacy Protection Act (15 U.S.C. §§ 6501, et seq.) (COPPA) and the Federal Trade Commission (FTC) Act (15 U.S.C. § 45, et seq.) COPPA requires website and online service operators to adhere to certain consent and notice requirements if they direct their platform to children under 13 or have actual knowledge they collect personal information online from children under 13. COPPA and its associated regulations and rules, increasingly enforced by the FTC, have received growing attention with the rise of popular applications amongst minors, including several legislative efforts to strengthen the statute. The FTC also has authority to enforce the FTC Act, which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce. The FTC has brought enforcement actions against organizations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information.

At the state level, the legal requirements are even more complex. While most states have their own version of COPPA and the FTC Act, others such as California and Illinois have adopted (or are considering) more robust and specific consumer privacy laws such as the California Consumer Privacy Act (Cal. Civ. Code § 1798.100, et seq.) (CCPA) and the Illinois Biometric Information Privacy Act (BIPA). The CCPA, for example, which took effect on January 1, 2020, provides most California residents the right to know what personal information has been collected about them, request that such information be deleted, and to opt-out of the sale of that information to third parties. The issue of a "sale" under the CCPA is particularly complicated because it involves the transfer or making available of personal information (which can include IP addresses in certain circumstances) for money or other valuable consideration. The CCPA imposes specific and significant obligations on covered businesses, applies extraterritorially, and carries with it the threat of potential penalties of $2,500 per violation and $7,500 per intentional violation. California voters approved a ballot measure to amend the CCPA on November 3, 2020, which will largely take effect on January 1, 2023. That ballot measure, known as the California Privacy Rights Act (CPRA) will greatly impact the eSports industry, with changes to how organizations process, retain, and obtain the consent of minors for the use of their data.

In addition to data privacy laws, there also exists a complex framework of information security standards in the US

that may impact eSports organizations. These laws generally require covered businesses to ensure that the personal information they collect is subject to reasonable security practices and procedures, including reasonable administrative, organizational, and technical safeguards. The CCPA, for example, only allows a private right of action if the California resident's personal information was compromised as a result of the failure of the business to maintain "reasonable" security measures. Although the CCPA does not define the phrase "reasonable security procedures and practices," the language is derived from another California law that predates the CCPA by almost 15 years. Under that law, the California Attorney General has opined that the California standard for reasonable security procedures and practices means, at a minimum, compliance with the Center for Internet Security's Critical Security Controls (CIS Controls). The CIS Controls largely map across to other well-information security frameworks, such as the NIST Framework (a widely accepted 2014 Cybersecurity Framework prepared by the US Department of Commerce's National Institute of Standards and Technology), the international security standards set forth by the International Standards Organization, and industry-specific frameworks such as the Common Security Framework developed by the Health Information Trust Alliance (HITRUST). In an industry involving multiple types of end-users, security challenges within the games themselves, and a diverse user base, determining what framework is applicable to a particular set of data, and then applying that framework consistently, can present numerous operational challenges for organizations in the eSports industry.

In short, data privacy and information security rules are becoming more complex in the US, and there is no "one-size-fits-all" approach for compliance. eSports organizations must therefore ensure their data strategies and compliance efforts align with the changing US legal landscape, and appropriately balance consumer data privacy with strategic growth goals. This means each organization must measure their legal requirements through the lens of their own risk tolerance and compliance structure. If they do it right, eSports organizations can help insulate against liability. If they do it strategically, they can position themselves to increase market share. If they do both, they may just win the game.

Your Key Contacts

Peter Stockburger
Partner, San Diego
D +1 619 595 8018
peter.stockburger@dentons.com