PRIVACY

With online and digital services becoming more commonplace in everyday life, the importance of protecting consumer data and privacy is critical. That is why the video game industry is committed to taking a number of affirmative steps to protect consumer privacy, including providing consumers with transparency, choice and control when it comes to managing personal information. Game publishers also believe in equipping parents and caregivers with information and tools to make informed decisions about how children can engage with video games, including the role of parents in helping to manage the collection of their children's personal information. Taken together, these efforts help create a safe, fun and customizable gameplay experience.

The Video Game Industry Leads in Protecting Children's Online Data Privacy and Safety

The video game industry employs several measures to comply with the Children's Online Privacy Protection Act (COPPA), such as:

- posting clear and comprehensive descriptions in applicable privacy policies of how data collected from children under 13 (U13) is handled;
- providing parents direct notice about information practices before collecting personal information from U13 children;
- obtaining verifiable parental consent before collecting any personal information from U13 children;
- giving parents the opportunity to review any personal information, revoke consent or delete personal information collected from their U13 children;
- implementing reasonable procedures to protect the security of U13 children's personal information.

In addition, the industry's authority for game ratings, the Entertainment Software Rating Board (ESRB), operates Privacy Certified, a privacy compliance and certification program approved by the U.S. Federal Trade Commission (FTC) to act as a Safe Harbor under COPPA. This program helps ensure that websites, mobile apps and connected toys and devices run by participating companies are compliant with applicable privacy laws as well as best practices.

Comprehensive Consumer Privacy Legislation Would Benefit Consumers

Consumers would benefit from a comprehensive consumer privacy law in the U.S. Congress should enact a consumer privacy law with clear and flexible standards as an alternative to the patchwork approach that has emerged among the states. Doing so would provide consumers with a consistent set of rights and expectations regardless of where they access online services.

PRIVACY (continued...)

The video game industry supports a framework that is compatible with the EU's General Data Protection Regulation (GDPR), an approach with which many ESA members already comply and which has served as a model for other countries.

Whatever framework is adopted—ideally at the federal level—it is critical that it include appropriate flexibility. The video game industry joins others in the business community in supporting a collection of consumer rights, including access, correction, deletion, portability and non-discrimination, subject to tailored and limited exceptions.

However, there are some nuances relevant to the video game industry that should be considered in any comprehensive approach:

- **Any New Laws or Regulations Concerning Children's Privacy Should Be Compatible with COPPA.** To the extent other privacy proposals cover children's data, it is important that they mirror the U13 age threshold for obtaining parental consent, as stipulated by COPPA and around which many companies have developed robust compliance programs over the years. If states were to adopt variable age thresholds, it would lead to a patchwork problem that would complicate effective compliance. The current U13 threshold is well calibrated. It is young enough to differentiate "child-directed" experiences from those directed at older teens and adults. Raising the age would make it considerably harder to maintain that distinction.
- **Non-Discrimination Clauses Should Be Sufficiently Flexible to Permit Free Online Games.** Free-to-play games are consistently among the most popular apps on mobile platforms. These games may be free to the player, but they are not free to make or operate. Publishers cover costs through a variety of means, such as tailored advertising or optional in-game purchases.

  To provide a customizable player experience, especially in mobile games, game publishers rely on data analysis and, to some extent, tailored advertising. The ability to gauge audience responses to the advertised products and services helps game publishers more effectively advertise and continue to offer such games for free or at a reduced cost to consumers.

  For that reason, non-discrimination provisions, which prohibit the data collector from declining service to consumers who refuse to share their personal data, should not be so rigid as to prevent ad-supported and similar business models. Absent that flexibility, free-to-play games, which are enormously popular with consumers, may become less prevalent in the marketplace, to the detriment of consumers.
- **Consumer Protection Laws Must Include a Fraud Exception.** Game publishers work diligently to ensure that all players can enjoy a game experience free from cheating, harassment, discrimination and fraud. Where inappropriate behavior arises, publishers take immediate steps to restore game integrity for the good of the game community. However, bad actors also take steps to subvert detection. For example, some players whose accounts have been suspended for cheating might use a "data access" right to try to determine how they were caught. Similarly, fraudsters may try to use the "deletion right" to force a publisher to digitally erase any evidence of who they are as well as any evidence of their misconduct. It should never be permissible for a bad actor to hijack legitimate consumer rights in a manner that would advance harmful conduct.

In circumstances where a game publisher has a reasonable belief that a bad actor is attempting to abuse a right in furtherance of a fraudulent act, the law should provide game publishers with the latitude necessary to protect other users. Accordingly, it is critical that consumer privacy laws include an exception applicable to fraud detection and policing related misconduct.

- **The U.S. Must Work to Replace the Privacy Shield Framework.** U.S. businesses were dealt a significant blow by the invalidation of the EU-U.S. Privacy Shield Framework by the Court of Justice of the European Union. This program provided a critical mechanism for complying with data protection requirements when transferring data between the U.S. and the EU. In essence, its regulations protected individual privacy while ensuring the continuity of commercial data transfers. While data transfers made pursuant to the standard contractual clauses are still possible, the U.S. and EU should work to replace the Privacy Shield with a more durable framework that will provide much-needed certainty for transatlantic data flows.