FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Business Blog

$20 million FTC settlement addresses Microsoft Xbox illegal collection of kids' data: A game changer for COPPA compliance

By: Lesley Fair | June 5, 2023

Care About COPPA Compliance may not be the coolest Xbox gamertag, but an FTC action against Microsoft for alleged violations of the Children's Online Privacy Protection Act Rule suggests it might be a good choice nonetheless. Filed by the Department of Justice on the FTC's behalf, the $20 million proposed settlement will require Microsoft to bolster privacy protections for kids who use its Xbox gaming system. The order also makes it clear that COPPA covers information like avatars generated from a child's image, biometric data, and health data collected with other personal information – and reminds businesses that the Rule imposes strict limitations on the retention of data from kids.

Used by millions of gamers – many of whom are under 13 – Microsoft's Xbox Live is an online gaming network that allows people to play through their Xbox Consoles. The FTC's action focuses on three ways in which Microsoft allegedly violated COPPA: 1) by collecting personal information from kids under 13 before notifying their parents and getting parental consent; 2) by failing to tell parents about the information the company collects from kids, why it's collecting that information, and the fact that it discloses some of the data to third parties; and 3) by retaining kids' personal information for longer than is reasonably necessary.

Where does the FTC say Microsoft went wrong? You'll want to read the complaint for details, but it started with the initial sign-up procedure. To play, users needed a Microsoft account. At the outset, Microsoft required them to provide their email address, their first and last name, and their date of birth. Until late 2021, Microsoft also asked for their phone number. What's more, Microsoft required them to consent to the company's service agreement, which until 2019 included a pre-checked box

allowing Microsoft to send them promotional messages and to share user data with advertisers. The sequence of events is important here because Microsoft asked for all that information even from users who had just told the company they were under 13. Only after gathering that raft of personal data from children did Microsoft get parents involved in the process. And that's at the crux of the FTC's allegation that the company violated COPPA.

To ensure that parents – not companies – are in control of information collected from kids online, COPPA requires two distinct forms of notice. The complaint alleges that Microsoft failed to comply with both mandatory provisions. Under Section 312.4(b) of the COPPA Rule – often called the **direct notice** requirement – a company must provide parents with direct notice of its information practices *before* it collects, uses, or discloses personal information from kids. The FTC says Microsoft violated that provision by collecting kids' names, email addresses, and phone numbers up front and only after that did the company notify parents and ask for their consent.

In addition, the FTC alleges Microsoft's direct notice was incomplete. Specifically, the notice didn't tell parents it would collect personal information beyond what the child had already provided – for example, kids' photos, their Xbox User ID, and other data the company combined with that ID. Another alleged deficiency: Microsoft simply told parents it collected, shared, and used information from kids, but then sent them to the Microsoft Privacy Statement to try to figure out the specifics for themselves. The FTC says what Microsoft should have done was describe its practices right then and there, rather than sending parents off on what amounted to a DIY errand.

Section 312.4(d) of the COPPA Rule – often called the **online notice** provision – requires (among other things) that companies post a prominent and clearly labeled link to an online privacy notice explaining their information practices "at each area of the Web site or online service where personal information is collected from children." The FTC says Microsoft fell short in complying with that provision, too. Until at least 2019, the required Privacy Statement discussed the company's practices in general, but didn't include what COPPA requires: the specifics about what personal information it collects from kids and its disclosure practices for that information. What's more, it didn't include a mandatory explanation for how parents can ask Microsoft to delete their child's personal information and to stop collecting it in the future.

The FTC alleges that by collecting personal information from kids under 13 before getting their parents involved, Microsoft violated Section 312.5 of COPPA. As that parental consent provision states, "An operator is required to obtain verifiable parental consent before any collection, use, or disclosure of personal information from children." Furthermore, the deficiencies in Microsoft's notice

compounded that violation. Put another way, how could parents' consent be effective if Microsoft didn't give them the information COPPA says is necessary for them to have before deciding whether to consent?

According to the complaint, Microsoft also violated COPPA's data retention and deletion requirements. According to Section 312.10, companies "shall retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected." After that, the company must securely delete the data. Here, though, Microsoft collected certain personal information from children during the account registration process, but even if the company ultimately didn't get parental consent, the FTC says that from 2015 until 2020, Microsoft held on to that data – often for years after the account creation process wasn't completed.

In addition to the $20 million civil penalty and injunctive provisions that have become standard in FTC COPPA cases, the proposed order will require Microsoft to implement new business practices to increase privacy protections for Xbox users under 13. Among other things, if parents haven't created a separate account for their kids, Microsoft must let them know that a separate account will provide additional privacy protections for their child by default. The company also must maintain a system to delete, within two weeks from the collection date, all personal information collected from kids for the purpose of getting parental consent unless the parent grants consent within that time. In addition, Microsoft must honor COPPA's date deletion requirements by getting rid of all other personal data collected from children after it's no longer needed. And if Microsoft discloses personal information about children to video game publishers, Microsoft must tell them the user is a child – a key provision that will put those publishers on notice that they, too, must apply COPPA protections to that child.

Here are some additional points that companies can take from the proposed settlement.

COPPA coverage is expansive. COPPA doesn't just cover websites and apps. It also applies to online services like Xbox. If you're part of the gaming ecosystem, are you current on what COPPA requires of your company? The FTC has resources to help your stay within the law.

COPPA's definition of "personal information" is broad. The proposed settlement with Microsoft sends a strong reminder to companies that the phrase "personal information" under COPPA covers much more than just a name or address. It also includes other information concerning the child or the parents of the child collected online from the child – for example, things like avatars, biometrics, vital signs, and health data, when collected and combined with other categories of personal information set forth in the Rule. With that compliance pointer in mind, take a closer look at the information yo

collect. (Also consider that as one more reason why you need to know about the FTC's recent Policy Statement on Biometric Information.)

Pay attention to what others are telling you about the sources of information. It's COPPA 101 that the law covers both websites and online services that are "directed to children" *and* those with "actual knowledge" they're dealing with data collected from kids under 13. So whether your company collected the information or you received the data knowing that someone else collected it from a kid under 13, the COPPA buck stops with you. Under the proposed order, that includes the video game publishers who must now be told by Microsoft when a user is under 13.

"Default," dear Brutus, is not in our stars, but in ourselves. A key takeaway is the importance of designing default settings with COPPA compliance in mind. Walk through your processes from the perspective of parents and kids.

Tags: Consumer Protection | Bureau of Consumer Protection | Privacy and Security | Children's Privacy

Leave a comment

Read Our Privacy Act Statement

Read Our Comment Policy

More from the Business Blog

Business Blog

Out of the mouths of babes? FTC says Amazon kept kids' Alexa voice data forever – even after parents ordered deletion

Lesley Fair | May 31, 2023

Business Blog

Not home alone: FTC says Ring's lax practices led to disturbing violations of users' privacy and security

Lesley Fair | May 31, 2023

Business Blog

Franchise Fundamentals: Taking a deep dive into the Franchise Disclosure Document

Lesley Fair | May 24, 2023

Business Blog

FTC public workshop on recyclable claims starts soon

Lesley Fair | May 23, 2023

Get Business Blog updates

Enter email address

Subscribe