WILMERHALE

FTC Brings First-Ever "Connected" Toys Privacy and Data Security Case; US, Canada, and Hong Kong Privacy Regulators Coordinate Enforcement

JANUARY 10, 2018

On January 8, 2018, the Federal Trade Commission (FTC) brought its first-ever privacy and data security case involving Internet-connected toys. VTech Electronics Limited and its US subsidiary (VTech), maker of Internet-connected portable learning devices, settled claims that it collected personal information from children without providing sufficient notice to parents or obtaining verifiable parental consent, as required by the Children's Online Privacy Protection Act (COPPA) and the FTC's COPPA Rule. The FTC also alleged that VTech failed to use reasonable data security measures to protect the information that it collected, pursuant to COPPA and the deception prong of Section 5 of the FTC Act. VTech agreed to pay $650,000 in civil penalties, implement a comprehensive data security program, engage in independent third-party audits every other year for the next 20 years, and comply with recordkeeping and reporting requirements.

In a sign that international privacy regulators increasingly are cooperating in their investigations and enforcement initiatives, the FTC stated that it had collaborated with the Office of the Privacy Commissioner of Canada (OPC), which released its own Report of Findings. OPC also collaborated with the Privacy Commissioner for Personal Data for Hong Kong—where VTech is headquartered—which in late 2015 initiated its own compliance check on VTech's data security practices.

COPPA Claims

The FTC's COPPA Rule ("Rule") applies to operators of commercial websites and online services (including mobile apps) directed to children under 13 that collect, use, or disclose personal information from children. It also applies to websites and online services that have actual knowledge that they collect personal information from children under 13. "Personal information" is defined broadly under the Rule to include information that directly identifies an individual, such as name and email address, as well as other information relating to the child, such as usernames, audio files containing the child's voice, photo or video files containing the child's image, or persistent identifiers such as cookie IDs, device IDs, or IP addresses.

FTC's allegation that VTech's Kid Connect app was an online service directed to children

According to the FTC's complaint, VTech provided educational products to parents and children through portable, Internet-connected electronic devices (known as "electronic learning products" or "ELPs") and various websites, mobile apps, and online platforms. One of the company's mobile apps, called "Kid Connect," could be used on the company's portable ELP devices to communicate with other children who used the Kid Connect app or with adults who downloaded the adult version of the app.

The FTC alleged that the Kid Connect app was an "online service directed to children" under COPPA. The FTC stated in its complaint that VTech's ELPs "are generally marketed as being appropriate for children ages 3 – 9," and that the company's Kid Connect app was a service that "is primarily intended to be used by children on Defendants' ELPs." Notably, the FTC concluded that the Kid Connect app was directed to children notwithstanding that:

- parents first needed to set up a Kid Connect account for each child and authorize the contacts with whom the child could communicate; and
- VTech's privacy policy, attached as Exhibit D to the FTC's complaint, appeared to state that "[a]lthough VTech sells and promotes children's products, all of our products are intended to be purchased by adults and the services offered by the Web Services are intended for adults."

The FTC appeared to focus on the fact that the company's portable ELP devices—and apps used on those devices—were allegedly marketed and intended to be used by children. Moreover, VTech allegedly did not have a mechanism in place to verify that the person registering the account was a parent and not a child, and in at least some circumstances had actual knowledge that children used its online services because it had collected children's birth date and year.

FTC's allegation that VTech did not comply with COPPA's notice and consent requirements when collecting information through the Kid Connect app

The FTC alleged that VTech collected personal information from children under the age of 13 through the Kid Connect app, including, "the content of text messages or messages to shared electronic bulletin boards, user names for a child that could be used to contact the child, and photographs and audio files containing a child's image or voice," as well as other information that was combined with information that could identify the child. However, VTech allegedly did not comply with COPPA's detailed notice and consent requirements, including by failing to:

- **provide sufficient notice on its website or online services of its information practices with regard to children (such as through a COPPA-compliant privacy policy that is clearly and prominently linked from the service's home or landing screen *and* at each area of the service where personal information is collected from children), in violation of Section 312.4(d) of the Rule;**
- **provide direct notice to parents of its information practices with regard to children, in violation of Sections 312.4(b) and (c) of the Rule; and**

- **obtain verifiable parental consent before any collection or use of personal information from children, in violation of Section 312.5 of the Rule.**

Accordingly, the FTC claimed that VTech violated the FTC's COPPA Rule.

Data Security Claims

The FTC also alleged that VTech failed to establish and maintain reasonable data security procedures to protect the information that it collected, as required under Section 312.8 of the COPPA Rule. According to the FTC's complaint, as a result of these security deficiencies, the company learned in November 2015 that a hacker had remotely accessed VTech's test environment, traversed into VTech's live environment, and accessed children's personal information. The compromised information allegedly included both clear-text data and encrypted data, but the hacker also allegedly accessed the database where decryption keys were stored.

The FTC alleged that the company failed to:

- **develop, implement, or maintain a comprehensive information security program;**
- **implement adequate safeguards and security measures to segment and protect VTech's live website environment from its test environment;**
- **implement an intrusion or prevention or detection system, or similar safeguards, to alert VTech of potentially unauthorized access to their computer network;**
- **implement a tool to monitor for unauthorized attempts to exfiltrate consumers' personal information across VTech's network boundaries;**
- **complete its vulnerability and penetration testing of environments that could be exploited to gain unauthorized access to consumers' personal information for well-known and reasonably foreseeable vulnerabilities, such as SQL Injection; and**
- **implement reasonable guidance or training for employees regarding data security and safeguarding consumers' personal information.**

The FTC also alleged that VTech's privacy policy stated that "in most cases," the information that VTech collected "will be transmitted encrypted to protect your privacy using HTTPS encryption technology," but that, in fact, VTech allegedly did not encrypt personal information that was submitted by users. The FTC therefore claimed that the company's representations regarding encryption were false and misleading and constituted a deceptive act or practice under Section 5 of the FTC Act.

Coordinated Enforcement Among International Privacy Regulators

The FTC also stated in its press release that it shared information and coordinated enforcement with the Office of the Privacy Commissioner of Canada (OPC) under the U.S. SAFE WEB Act. Jacqueline Connor, an FTC staff attorney and lead FTC lawyer on the case, reportedly stated that "[a]s consumers around the world adopt new technologies, they increasingly share personal information with companies that operate globally. Therefore, it is crucial that the FTC cooperates

with its foreign partners in enforcing privacy and security laws."

The OPC also reportedly exchanged information and analysis with the FTC, and OPC indicated that it had issued a Report of Findings, instead of requiring its own compliance agreement, because VTech had already made binding commitments in its settlement with the FTC. The OPC stated that it also had worked with the Privacy Commissioner for Personal Data for Hong Kong, where VTech is headquartered, which demonstrates that international privacy regulators are increasingly coordinating their investigation and enforcement efforts.

Implications for Businesses

Acting FTC Chairman Maureen K. Ohlhausen emphasized in a statement that **"[a]s connected toys become increasingly popular, it's more important than ever that companies let parents know how their kids' data is collected and used and that they take reasonable steps to secure that data."** Importantly, the FTC may seek **civil penalties of up to $40,654 *per violation (e.g., per COPPA Rule violation, per child)*** under COPPA, so it is imperative that companies take steps to ensure they comply with ***all*** requirements under the FTC's COPPA Rule.

Companies should review the FTC's Complying with COPPA: Frequently Asked Questions and follow the FTC's six-step compliance plan for businesses, summarized below:

1. **Determine if your company is a website or online service (including mobile apps, Internet-connected devices, and other online services) that collects personal information from children under the age of 13;**
2. **Post a privacy policy that complies with COPPA and the COPPA Rule (and include clear and prominent links to the privacy policy on the home or landing screen *and* at each area of the service where personal information is collected from children under the age of 13);**
3. **Notify parents directly, as required by COPPA and the FTC's COPPA Rule before collecting personal information from their children under the age of 13;**
4. **Get parents' verifiable consent before collecting personal information from such children;**
5. **Honor parents' ongoing rights with respect to personal information collected from their kids; and**
6. **Implement reasonable procedures to protect the security of kids' personal information.**