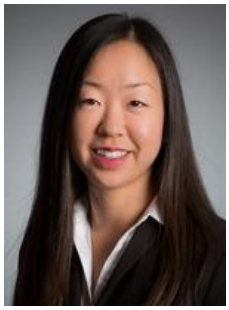
Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

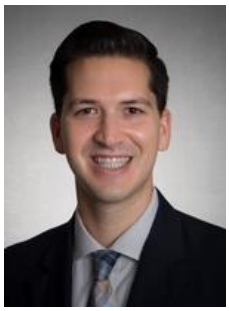
Digital Toy Data Breach Highlights Cybersecurity Concerns

By **Erin Bosman, Julie Park and Benjamin Kagel** (June 5, 2018, 4:01 PM EDT)

Erin Bosman



Julie Park



Benjamin Kagel

For the second time, an Illinois federal judge powered down a proposed class action against VTech Electronics, following a 2015 data breach of its internet-connected digital learning toys. The data breach also triggered separate allegations by the Federal Trade Commission that VTech violated federal children's privacy laws.

Both developments illustrate the increasing exposure that the internet of things brings when consumer product manufacturers collect and store consumers' personal data with connected devices. They also demonstrate how the need to address these issues up front is imperative.

Toy Data Breach Claims Dismissed Again

In In re VTech Data Breach Litigation, the plaintiffs sought to represent a class of consumers who purchased VTech's digital learning devices. Their claims arose after a hacker lifted personally identifiable information affecting 4.8 million adult accounts and 6.3 million child profiles linked to the devices. The plaintiffs claimed that VTech broke promises to consumers because of alleged inadequate data protection measures and subsequent suspension of online services accompanying the devices.

The court disagreed. It had dismissed the suit once before on multiple grounds, including lack of standing to show future harm and failure to state a claim. In granting VTech's motion to dismiss a second time, the court rejected the plaintiffs' arguments that VTech spurned any implied promises it made to consumers at the time of purchase.

The court reasoned that the alleged promises must be controlled by the express terms and conditions consumers agreed to when first using VTech's online services post-sale. When consumers buy the device, they cannot access its online features until they create an account and expressly agree to VTech's online services terms and conditions. The terms governing the device's internet features also incorporate a privacy policy that promises to keep consumers' data secure.

The plaintiffs' complaint asserted a breach of contract claim based on an implied contract at the point of

purchase. The court found this insufficient, and dismissed the claim because the plaintiffs failed to allege that VTech breached the express online service terms or the incorporated privacy policy.

The plaintiffs also asserted that VTech's online service suspension rendered the toy devices essentially useless, in breach of the implied warranty of merchantability. VTech countered that the plaintiffs could not show that anything was actually wrong with the toys themselves or that users could never access the online services. The court agreed with VTech, finding these pleading defects fatal to the plaintiffs' claim.

Finally, the court dismissed without prejudice the plaintiffs' remaining allegations for unfair and deceptive business practices, for failing to meet the heightened pleading requirement for fraud-based claims, and dismissed the unjust enrichment claims on choice-of-law grounds.

FTC COPPA Action First To Involve Kid's Connected Devices

While the proposed class action sat in Illinois district court, the FTC filed a complaint against VTech in the FTC's first children's privacy case involving connected toy products under the Children's Online Privacy Protection Act.

Under COPPA, companies that collect personal information online from children under 13 must take reasonable steps to protect children's data, including providing direct notice to parents that the device collects such information and obtaining their consent. The FTC claimed VTech failed to take these steps. The FTC also alleged that VTech's privacy policy falsely stated that consumers' personal information would be encrypted when in fact it was not.

VTech settled with the FTC for $650,000, and agreed to implement a comprehensive data security program to ensure future compliance with COPPA and to protect consumers' personal information.

Following the VTech settlement, the FTC flexed its regulatory arm internationally when it sent warning letters to two foreign app developers. The letters notified the companies that their collection of children's geolocation data without parental consent may violate COPPA. The agency stressed that the letters were meant to send a message that the COPPA rule applies to any company that targets children in the U.S.

In light of this foreign enforcement activity, internet of things companies should consider running COPPA compliance checks not only on their domestic services but also on any affiliated foreign-based websites or online services that collect personal information from children in the U.S.

Implementing Effective Cybersecurity

Although VTech's case came with a relatively favorable outcome, it highlights the importance of implementing sound data privacy and security measures in internet-connected consumer devices, as courts, federal regulators and industry leaders grapple with the interplay between cybersecurity and product liability.

While many federal agencies exercise authority that touch on privacy and data security issues, no single agency or law covers the collection and use of personal data.

For instance, the U.S. Consumer Product Safety Commission is the regulatory agency traditionally

responsible for protecting the public from hazards associated with consumer products. Yet, even as internet-connected products spread to more and more households, the CPSC does not consider personal data security and privacy issues to be consumer product hazards under its jurisdiction.

The CPSC held a public hearing on May 16, 2018, to discuss potential safety issues and hazards associated with internet of things consumer products. Whether the hearing will change the CPSC's traditional definitions of consumer hazards remains to be seen.

The FTC has brought numerous privacy-related enforcement actions against companies, including allegations related to unauthorized disclosure of personal data, unlawful use and disclosure of financial information, failure to comply with posted privacy policies and other consumer protection laws that raise data privacy issues. Nonetheless, internet-connected consumer products remain in a regulatory gray area when data breach incidents arise.

As VTech's case demonstrates, courts continue to rely on traditional notions of contract law, state consumer protection laws and product liability when assessing a company's liability for data privacy issues involving its connected devices. Because a cybersecurity flaw in an internet of things product does not necessarily constitute a product defect, courts look instead to the promises a company makes to consumers as a basis for liability. Such promises tend to materialize via the product's marketing, packaging and labeling, and terms and conditions.

The internet of things unlocks new potential for consumers and businesses to enhance productivity, improve efficiency and fuel innovation. But it also breeds privacy and data concerns. To realize the benefits and avoid the pitfalls, connected device manufacturers should evaluate their cybersecurity measures and consider investing in robust data protection measures.

As they continue to innovate and place new internet-connected consumer products on the market, internet of things companies face increasing litigation risk from data breaches, privacy-related claims and regulatory enforcement actions. Bringing in specialists to address these issues before they arise will reduce the inherent risks associated with connected consumer products.

Erin M. Bosman and Julie Y. Park are partners and Benjamin S. Kagel is an associate at Morrison & Foerster LLP.

[1] In re VTech Data Breach Litigation, Case No. 1:15-cv-10889 (N.D. Ill. 2018).