PAUL HASTINGS

STAY CURRENT

January 2018

Follow @Paul_Hastings

Key Takeaways from the FTC's Latest Privacy Enforcement

By Behnam Dayanim, Robert Silvers, Sherrese Smith & Edward George

On January 8, the Federal Trade Commission ("FTC") settled allegations with VTech, an electronic toy maker, for violations of the Children's Online Privacy Protection Act ("COPPA") and for failing to use reasonable and appropriate data security measures to protect its customers' personal information. The enforcement action, resulting in fines of over $650,000, is the latest reminder that companies can expect the consumer protection agency to closely scrutinize the privacy and cybersecurity protections in the connected devices and platforms that make up the Internet of Things ("IoT").

The FTC's complaint alleged that the Kid Connect app, used with certain VTech electronic toys, collected the personal information of hundreds of thousands of children. The problem? The FTC alleged that VTech failed to provide direct notice to parents or obtain verifiable-consent from parents concerning its information collection practices. COPPA prohibits the collection of personal information from children thirteen and under unless a company:

1. Provides sufficient notice on its website or online service about the information collected, how the information is used, and its disclosure practices;

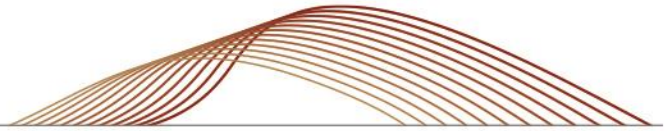
2. Provides direct notice to parents of the information collected, how the information is used, and its disclosure practices;

3. Obtains verifiable parental consent before any collection or use of personal information from children occurs; and

4. Establishes and maintains reasonable procedures to protect the confidentiality, security, and integrity of the children's personal information collected.

The FTC also alleged that VTech violated Section 5(a) of the Federal Trade Commission Act when VTech stated in its marketing materials for Learning Lodge, a platform similar to an app store that parents had to register with before their kids could access the Kid Connect app, and Planet VTech, a web-based gaming platform for children ages "5+", that all personal information submitted to the platforms by consumers would be transmitted in encrypted form, when in fact it was not.

Up close, VTech is significant because it is the first children's privacy case that involves Internet-connected toys, but, taking a step back, this enforcement action is just the latest in a string of recent regulatory pronouncements related to the IoT and related corporate cybersecurity practices. VTech, combined with the FTC's enforcement actions in *Wyndham* in 2015 and VIZIO in 2016, suggests that



the FTC will be maintaining its approach to enforcement actions under the Trump Administration, at least with respect to privacy and cybersecurity practices.

Wyndham was significant because not only was the FTC's authority to regulate data security validated by the Third Circuit, the FTC's message to companies holding personal data seemed rather clear: certain steps (complex passwords, vendor management, systems inventory, and incident response protocols) are always expected, and, once a company becomes aware its network is vulnerable, it is imperative the company takes steps to address those vulnerabilities promptly and effectively.

VIZIO is significant because the FTC interpreted its Section 5 unfairness prong in a broad way. Specifically, the FTC alleged that VIZIO used the technology to "comprehensively collect the sensitive television viewing activity of consumers or households" and deemed that tracking "unfair." This was the first time the FTC labeled television viewing activity as sensitive information. The FTC alleged that the collection and sharing of this sensitive information without the consumers' consent had caused, or is likely to cause, substantial injury to the consumer.

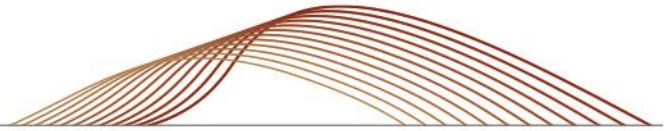
Crystal balls are always perilous; however, in this case, some predictions are easy to venture. The FTC is going to continue to pursue privacy and cybersecurity cases where it perceives corporate negligence, inattention, or deception. Companies need to take the opportunity to review or develop the appropriate policies and safeguards to handle personal information. Key to all of this will be reasoned, deliberate decision-making in establishing key policies and procedures. That, in turn, requires several key steps:

- Understand what information you are holding and where it is located. Until you know what you have and where it is kept, it is impossible to know what measures may be needed to protect it.

- Assess the information's **legal** and **commercial** sensitivity. Understand the statutory and regulatory requirements that attach to the information you hold, and also assess its business importance. It is impossible to protect all data equally well. Value judgments must be made, and differing levels of security ascribed based on both legal and business requirements. Both factors are critical. Reliance on either alone would be incomplete and create substantial potential exposure to loss.

- Manage your vendors. Know who they are and what they can access. Make deliberate decisions in determining the extent and duration of that access, limiting it only to what is needed for them to perform their designated functions.

- Lastly, incident notification and remediation are critical. In the already notorious Equifax breach, part of the public opprobrium focused on Equifax's perceived ineptness in addressing the incident after it occurred — its failure to communicate internally to key stakeholders (possibly resulting in sales of shares by senior executives after the breach had occurred) and the length of time after the breach before the company began notifying consumers. Delays sometimes are inevitable, as companies attempt to figure out the scope and contours of a breach, but regulators are increasingly demanding prompt notifications. Already, for example, the New York Department of Financial Services requires notice to the agency within 72 hours of a breach,[1] and the new European General Data Protection Regulation imposes the same time frame.[2] As of this writing, Congress is considering national breach notification legislation, and several states are proposing to tighten their existing requirements.



Clear lines of authority and accurate understanding of systems and data are essential to timely and appropriate incident response. The only way to have confidence that a process will work is to test and test again. Companies that do not "table-top" their incident response programs risk unforeseen delays and inaccuracies when responding to a breach.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings Washington, D.C. lawyers:

Behnam Dayanim
1.202.551.1737
bdayanim@paulhastings.com

Robert P. Silvers
1.202.551.1216
robertsilvers@paulhastings.commailto:attorney@paulhastings.com

Sherrese M. Smith
1.202.551.1965
sherresesmith@paulhastings.com

[1] N.Y. Comp. Codes R. & Regs. tit. 23 § 500.17.

[2] Commission Regulation 2016/679, 2016 O.J. (L 119) 1, art. 33 (EU).