IoT meets VR: The Next Concern Over Mobile Privacy

BY ADAM GRANT

In the beginning of this year at the Consumer Electronics Show in Las Vegas, it seemed as if every sponsor and vendor was introducing a product that demonstrated a deep commitment to mobile technology and its interaction with the "Internet of Things." Clearly, 2014 appeared to be the year mobile technology would move from a consumer's interaction only with their mobile device, to a consumer's interaction with their physical environment using their mobile device. In my January article I discussed the amazing new ideas and how privacy concerns eked into the many different aspects of this new technology.

However, on March 25, 2014, the year took a dramatic shift with the introduction of a new platform for mobile. On that day, Mark Zuckerberg announced Facebook's acquisition of Oculus VR. In the announcement, Zuckerberg stated: "Our mission is to make the world more open and connected. For the past few years, this has mostly meant building mobile apps that help you share with the people you care about. We have a lot more to do on mobile, but at this point we feel we're in a position where we can start focusing on what platforms will come next to enable even more useful, entertaining and personal experiences.

This is where Oculus comes in. They build virtual reality technology, like the Oculus Rift headset. When you put it on, you enter a completely immersive computer-generated environment, like a game or a movie scene or a place far away. The incredible thing about the technology is that you feel like you're actually present in another place with other people. People who try it say it's different from anything they've ever experienced in their lives."

According to Zuckerberg, gaming will be the initial focus of VR (virtual reality). Immediately, this brings into focus the disclosures necessary to engage in these games if personal identifiable information is being obtained. Immediately after the announcement, Oculus fans apparently reacted in a manner that could only be characterized as anything but positive. It has been reported that early backers of Oculus VR are extremely mad at CEO and founder Palmer Luckey. The backers apparently believe that Facebook will destroy the Oculus vision for VR. They believe that Facebook will mine all their data and harass them with advertisements.

Merging the worlds of IoT and VR, even if the technology only reaches the gaming community, means a whole new world of privacy related issues must be explored and properly addressed to avoid liability. The intersection of these technologies leads to endless questions and concerns, but as the initial push appears to be the gaming industry, it is important to understand the concerns in relation to the Child Online Privacy Protection Act. (COPPA)

Does COPPA apply to VR technology? Initially, COPPA specifically applied to operators of websites or online services. However, in July 2013, the FTC announced it expanded the scope of COPPA, "The definition of a website or online service directed to children is expanded to include plug-ins or ad networks that have actual knowledge that they are collecting personal information through a child-directed website or online service. In addition, in contrast to sites and services whose primary target audience is children, and who must presume all users are children, sites and services that target children only as a secondary audience or to a lesser degree may differentiate among users, and will be required to provide notice and obtain parental consent only for those users who identify themselves as being younger than 13."

According to an April 2014 release by the Bureau of Consumer Protection Business Center and the FTC, "online services" include mobile apps. Thus, based on the expanded definition of the rule which includes plug-ins that collect PII and the use of a mobile device to interact with the VR unit, we can anticipate that the FTC will take the position that the Oculus headset operating system will likely need to comply with the COPPA requirements.

Another interesting issue is whether California's Attorney General Kamala Harris will take the position that a privacy notice on Facebook's website will be sufficient to apply to an individual who uses the headset, or whether the headset will need to have a privacy notice embedded in the VR experience.

According to the lawsuit filed by AG Harris against Delta Airlines for its "Fly Delta" app, referring to a website's online privacy notice is insufficient to cover a mobile device. Thus, based on this argument, which is currently up on appeal, Mr. Zuckerberg may face an uphill battle if he relies only on the Facebook privacy notice.

The expanded definition of PII seems to also include information the VR apparatus would likely collect. For example, PII for purposes of COPPA, now includes; A photograph, video, or audio file, where such file contains a child's image or voice; Geolocation information sufficient to identify street name and name of a city or town; or Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described above. Clearly, the expanded opportunities of collecting PII through VR is both a treasure trove and a challenge. All of this information can easily be collected during a VR experience.

The real challenge in requiring VR technology to comply with COPPA will be the interplay between functionality and legal compliance. COPPA requires that parent's ability to interact with the site and change or delete the child's information. However, just how a developer is going to be able to achieve such access and ability while keeping the "virtual" feel in place will be a challenge. In particular, if the software requires and "just in time" privacy notice, then the entire experience will likely be lost in legalese.

So, barely half way through 2014 and we are faced with a new twist with the direction of mobile technology. In the beginning of the year we anticipated being drawn into the expanding "web" of the Internet of things and now we are leap frogged past that concept into a new virtual reality.

Adam is a principal with Alpert,Barr & Grant, APLC, and has nearly 20 years of legal experience. His practice focuses on all forms of civil litigation including mobile app laws with a clear understanding of the fast-changing landscape of data privacy, Adam regularly advises app developers and businesses with an online presence on how toeffectively deal with the issues on data collection and analysis. He helps developers andbusinesses avoid entering a legal maze with no exit.