Bloomberg Law

Privacy and Security Law Report®

Biometrics

Privacy Issues in Virtual Reality: Eye Tracking Technology

Eye Tracking

Companies are pursuing user eye-focus tracking to control virtual reality interfaces. The technology may enhance user experience and efficiency, but eye tracking also has applications that may have privacy legal and regulatory implications that VR headset makers, content creators, and advertisers need to be aware of, the author writes.

BY BHAVISHYA RAVI

Virtual reality (VR) is poised for widespread adoption and promises to be a $40 billion industry by 2020. There has been an increase in VR content, with several players exploring virtual and augmented reality solutions.

Companies creating VR devices have explored various means of user interaction: voice, motion controls (e.g., smart gloves) and handheld devices (e.g., joysticks). While these methods offer some benefits, they fail to create a truly immersive experience.

That brings us to eye tracking. Companies are pursuing the idea of enabling a user's natural gaze to control interactions with the VR interface. A user's gaze is also being employed for ''foveated rendering.'' This is a technique where a user's natural gaze renders the VR experience only within the area of the eyes' focus. This greatly reduces the workload for the device and enhances the experience.

Eye-tracking technology has the potential to significantly enhance user experience and enable VR in a manner that physical control devices cannot. However, considering the nature of information that can be gleaned from eye-tracking data, there may be regulatory risks in collecting and using such data.

Bhavishya Ravi is a senior associate on the Technology & Privacy Team at Alston & Bird LLP in Los Angeles.

What is Eyetracking? Eye tracking is not entirely new. It has been attempted since (at least) the early 1900s to study reading. In the 1980s, market researchers used eye tracking to assess the efficacy of advertisements. For several years now, consumer-facing technology companies have regularly used eye tracking to assess user behavior while testing their products.

Eye tracking is commonly accomplished by employing near-infrared technology along with a high resolution camera to track a person's gaze. In this process, the light is directed toward the center of the eyes, creating reflections in the cornea. These reflections are tracked using a camera. This technology can determine the places on a document or image that your eyes fixated on (''gaze points''), the amount of time spent in those places, if the eyes locked toward a specific object (''fixation'') and the movements from one fixation to another (also known as ''saccades'').

What Can Eye Tracking Find Out About You? The fixation points and the saccades are good measures of visual attention and interest. Researchers can create heat maps by aggregating the gaze points and fixations to show the areas a person showed heightened interest in. Fixation sequences track the various points that the eye fixed on, the time spent on one and the time that it took to fixate on another point—telling you what a person looked at in a particular image or document and the sequence of attention. In addition, if the tracker collects pupil dilation, it can potentially assess a person's mental and emotional state.

 ISSN 1538-3423

Gaze data, similar to fingerprints, is unique for every individual and can be used to identify individuals or as a password. While typically gaze data has to be previously recorded and associated with a person's identity, research indicates that even if gaze data was not previously stored and identified as belonging to someone, it is possible to use attributes from gaze patterns to approximate the identity.

A person's gaze can suggest a person's age and gender, while pupil dilation can predict sexual orientation. It can also detect or aid in the diagnosis of health conditions.

Proposed and Potential Applications of Eye Tracking While user experience and foveated rendering are the most commonly cited reasons for using eye tracking in VR, there are other applications. Since gaze data uniquely identifies individuals, it is possible to use it as an authentication mechanism or as a password. In fact, researchers have argued that eye-tracking biometrics can protect against spoofing that is a concern with iris scans. In addition, researchers have found that this can be used to seamlessly and continuously authenticate a user. While current commercial applications do not offer this feature, the technology is progressing towards a level of accuracy that makes this commercially feasible. For advertisers, eye tracking can be an accurate metric to assess attention and interest. Using this information, advertisers could optimally place and design advertisements. For content creators, tracking a person's gaze can tell which parts of the content generated interest and the emotions it elicited. In fact, instead of being just a tool of interaction, gaze tracking can be used to glean a user's eye movement and emotions to create and depict expressive avatars in the virtual world. For healthcare providers, eye-tracking data of their patients can aid diagnosis of new conditions or monitoring of existing conditions.

Regulatory Standards The U.S. has not adopted comprehensive privacy laws at the federal level. Instead, it has enacted sector-specific or data-specific laws. For example, there are provisions that regulate personal information in the financial industry. Similarly, there are laws specifically applicable to children's personal information, health information, biometric information and video viewership information. In addition to such specific laws, the Federal Trade Commission (FTC) has emerged as the primary regulator in this area. Section 5 of the FTC Act imposes a general obligation on companies to not engage in ''unfair and deceptive'' trade practices. The FTC has used its powers to initiate enforcement actions under Section 5 against companies for deceptive privacy policies and unfair data collection/use practices.

In its various enforcement actions, the FTC has indicated that collection of persistent identifiers such as IP addresses, unique IDs, MAC addresses, device IDs, or similar uniquely identifying data must be disclosed to users. In its guidance, it has opined that any data that is ''reasonably linkable'' to an individual can constitute personally identifiable information. The FTC's staff has also indicated that probabilistic tracking, i.e., aggregating or using different data points to determine the user of that device, is required to be truthfully disclosed while offering meaningful options to the user to opt out of such tracking. While its enforcement actions do not expressly include eye-tracking data, considering the ability of such data to uniquely identify an individual by itself or with other data elements, it may be treated as personally identifiable information.

Eye tracking can also identify with specificity what a user viewed, the manner of viewing and the duration—all indicators of the user's interest or preferences, which in turn can inform behavioral advertising. In enforcement actions involving behavioral advertising, the FTC has required companies tracking user behavior to provide a prominent disclosure with an option for users to opt out of such tracking. Some companies have been required to also disclose the technologies and methods used for targeted advertising. If eye tracking is going to be used for advertising and behavioral tracking purposes, it is a best practice to provide notice to users about such tracking and the mechanism employed—and offer a meaningful opt-out choice.

Using eye-tracking data for authentication relies on unique physical characteristics of an individual, i.e., biometric information. When commercial applications begin reliably authenticating a person, FTC guidance and state laws on biometrics will apply to the collection, processing and use of such data. The FTC staff report Best Practices for Common Uses of Facial Recognition Technologies recommended providing consumers with meaningful choice, employing reasonable security protections, appropriate retention and disposal practices, and being transparent about privacy practices around biometric data. Washington recently enacted a law on biometric identifiers and became the third state after Illinois and Texas to regulate biometric information. This law defines a biometric identifier to mean data generated by *automatic measurements of an individual's biological characteristics* such as fingerprints, voiceprints, eye retinas, irises, or *other unique biological patterns or characteristics* that is used to identify a specific individual. Eye-tracking data can potentially fall under this definition. Companies that capture, process and store such biometric identifiers while matching or connecting them to individuals have to provide notice, obtain consent, or provide options to opt out to such individuals. Disclosure of such datasets typically requires user consent unless the exceptions outlined under the law become applicable. In addition, there are obligations to exercise reasonable care to guard against unauthorized access and not retain the data for longer than reasonably necessary. While Illinois and Texas also have laws on biometric data, their definitions are specific to certain datasets and may not be applicable in this context. If there is a security breach that impacts biometric data, data breach obligations may be triggered in Illinois, Maryland, Nebraska, New Mexico, Iowa, North Carolina, Wyoming, and Wisconsin depending on the other datasets at issue and whether the datasets were encrypted or redacted.

Another consequence of detecting how the user engaged with audio-visual material displayed on a VR headset is that the Video Privacy Protection Act (VPPA) may apply to such data. The law's definition of ''personally identifiable information'' includes information that identifies a person who has requested or obtained specific video materials or services from a video service provider. This term's interpretation has differed depending on the jurisdiction considering the matter. In very simple terms, under the majority (more commonly adopted) approach, a court would not consider unique IDs or data that requires other data along with it to link

  PVLR ISSN 1538-3423

an actual person to video materials as personally identifiable information. Since eye-tracking data typically would require a match or search on a database to conclusively confirm an identity, this may not be considered personally identifiable information. Whereas under the minority (less commonly adopted) approach, any unique identifier that could enable re-identification with other data sets would qualify as personally identifiable information. In a jurisdiction that follows this approach, it may be possible for plaintiffs to argue that this is personally identifiable information. Since the law *and* the technology are evolving in this area, this analysis needs to be revisited with new developments.

Interestingly, the FTC recently initiated its first enforcement action relating to video viewership and privacy. While the VPPA's protection only extends to disclosure of video viewing data, this enforcement action also related to the *collection* of video viewing data. A television manufacturer had tracked its users' television viewing activity by using automatic content recognition technology to identify the content they were watching. The FTC alleged that the data was sensitive and that the collection of such data was an unfair practice. While this case is the first of its kind and relates to a smart television provider, VR headset manufacturers must take note of this enforcement while building functionality that enables user identification and content recognition.

Conclusions Eye tracking promises to change the way we interact with devices. The technology has various applications, including enhancing user experience and efficiency. However, eye tracking also has applications that may have privacy implications. Although this is a new and growing technology, VR headset makers, content creators, and advertisers need to be aware of how the existing frameworks of law and regulatory guidance could apply to them. As a best practice, entities in this space can consider the following: using privacy notices, obtaining user consent when sensitive identifying data is being collected or shared, providing users with meaningful choice, employing reasonable security practices including encryption, and acting in line with the representations made in privacy notices and user expectations.