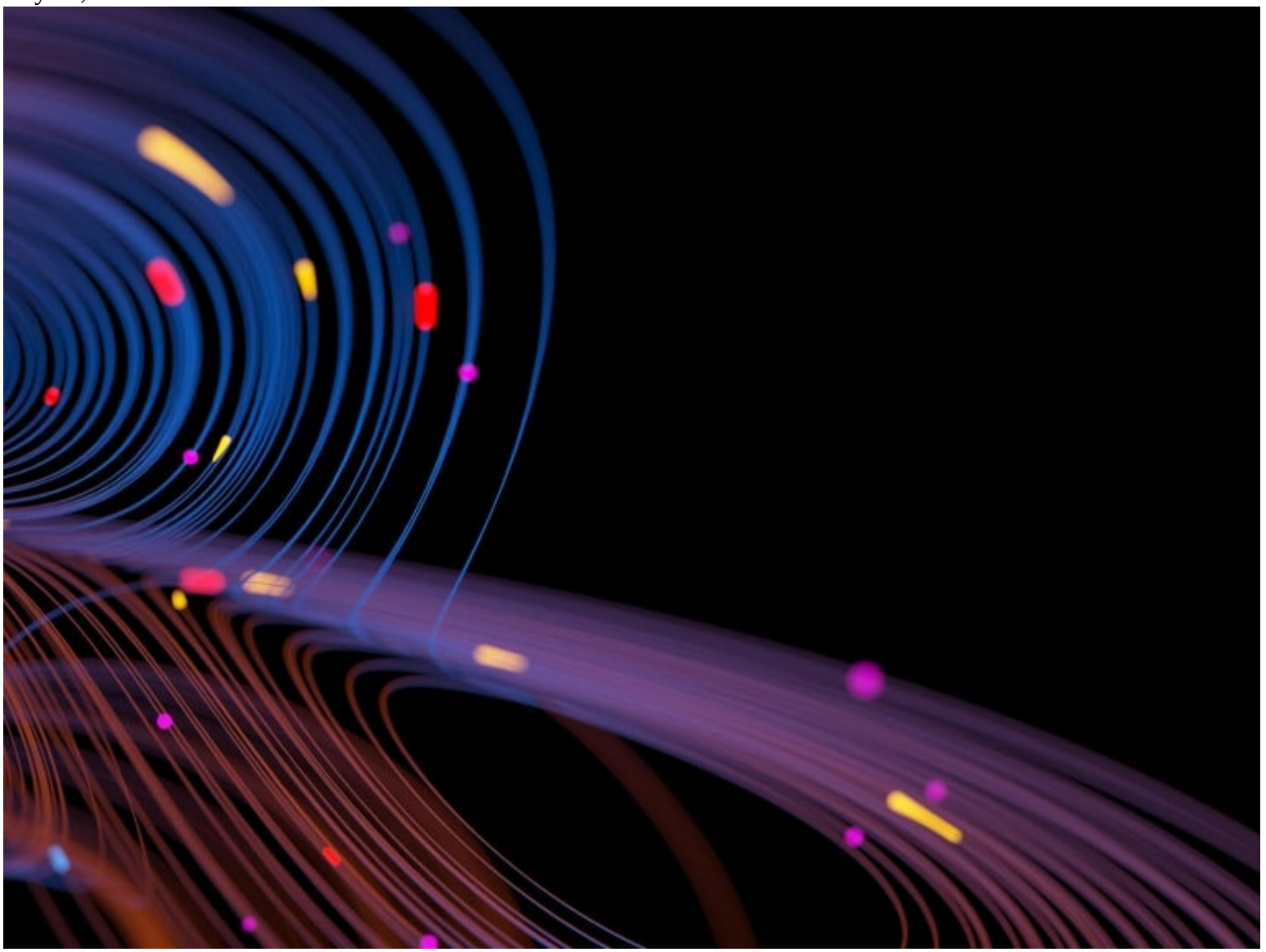
Blogs
July 16, 2024



In the contemporary digital ecosystem, the lines between personalization and privacy often blur, specifically when involving advanced technologies such as gaze and eye tracking. As we interact with various technologies from smartphones to AR devices, our gaze becomes a valuable metric, one that could enhance user experience but also raise significant privacy concerns.

The Value of a Gaze

The human gaze is an extraordinary indicator of interest, intent, and emotion. With advancements in gaze tracking technology, companies have unearthed a gold mine of data that provides profound insights into user

behavior. The ability to discern where a user is looking—their gaze pattern—is not only an engineering marvel but also a vital tool for enhancing user experiences and creating targeted marketing strategies.

Eye Tracking Technology in Modern Devices

The integration of eye tracking in devices such as the Apple Vision Pro has propelled the potential of user engagement metrics to new heights. This integration allows for a nuanced understanding of how users interact with a device. When a user's gaze lingers on a specific part of the screen, it indicates interest or engagement with the content presented. Conversely, if a gaze quickly flits away, it might suggest disinterest or dissatisfaction.

By harnessing this information, companies can optimize user interfaces, streamlining the user experience by bringing frequently accessed features to the forefront, minimizing friction, and enhancing the overall aesthetic appeal. In addition, this data aids in constructing dynamic content that adapts to the user's interests, keeping them engaged and invested in the platform they are using.

The true value of gaze data goes beyond mere interface optimization. A user's gaze pattern can act as a window into their subconscious preferences. It can reveal preferences that the user may not be explicitly aware of, leading to insights that traditional feedback mechanisms might not uncover.

For example, while reading an article online, the sections upon which a reader's gaze lingers could reveal which arguments resonate with them, which data they find most convincing, or which narratives evoke an emotional response. Such data is priceless for content creators, enabling them to tailor content to their audience's latent preferences.

Furthermore, gaze patterns can reveal information about a person's biases, beliefs, or interests. This level of detail provides a unique opportunity for personalized content delivery but also raises questions about the ethical implications of such personalized targeting and possibly legal obligations regarding the processing of sensitive personal information.

The Multifaceted Value for Advertisers and Marketers

For advertisers and marketers, knowing where a user's attention naturally gravitates can inform ad placement, design, and content. This can lead to higher engagement rates and, ultimately, a more significant return on investment.

Advertisers can pinpoint what captures attention in an ad—be it a headline, an image, or a particular color scheme—and tweak their creative elements accordingly. The result is advertising that is more engaging as it aligns more closely with the user's natural interests and behaviors.

The intricate value of a gaze within the digital landscape is multifaceted and far-reaching. As eye tracking technology evolves and becomes more precise, its applications will expand, providing even deeper levels of interaction and personalization. These exciting opportunities also bring with them the need to understand the privacy implications of processing gaze data.

Privacy Implications

The technological marvel of gaze tracking is not without its profound privacy implications. As devices become capable of capturing and interpreting our gaze with increasing accuracy, a significant assessment of how data is collected, used, stored, and disclosed is critical to identifying applicable legal requirements, which may include notice, consent, privacy impact assessments, security measures, and limits on processing, retention, and transfers. These requirements may arise from collection of eye data, but they also may arise from additional

personal information derived from gaze tracking, such as inferences about the individual's alertness, age, gender, or physical or mental health. Gaze tracking can also be used to infer an individual's preferences, such as for shopping or content, which can generate further inferences about them, such as their political affiliations or sexual orientation. Depending on how gaze data is collected and used, it may trigger heightened obligations commensurate with that of financial records or health information.

The Evolving Legal Landscape

While existing privacy and biometric laws address biometric data, they tend to define this term broadly and do not explicitly refer to gaze tracking. But there is some indication that courts are considering whether gaze data specifically falls under the scope of these laws. For example, the Illinois Biometric Information Privacy Act (BIPA) defines biometric identifier to include, in relevant part, a retina or iris scan. Courts have started to contemplate whether gaze data falls within this scope in series of cases involving remote exam proctoring services. Federal regulators are also recognizing that biometric data involves more than static collection of data. In its 2023 Biometric Policy Statement, the Federal Trade Commission (FTC) states its view that biometric information includes, in relevant part, descriptions or recordings of an individual's characteristic movements.

Further clarity is likely to come in the course of BIPA litigation and regulator enforcement. As such, it is ever more important to work with knowledgeable privacy and regulatory counsel that can help guide companies as they use gaze data to ensure that they are implementing best practices.

Consent and Control

The European Union's General Data Protection Regulation (GDPR) started a wave of new privacy legislation across the globe. While the frameworks of these laws vary, most generally state that individuals have a certain level of control over their personal information and require consent for the processing of sensitive personal information, such as biometric data and data revealing political opinions or sexual orientation. Many U.S. state privacy laws also require providing opt outs from selling or sharing personal information for behavioral advertising purposes or from using personal information for automated decision-making. While stopping short of requiring consent for processing biometric information, the FTC's Biometric Policy Statement stressed the need for clearly and conspicuously disclosing the collection and use of biometric information and stated that failing to do so may violate Section 5 of the FTC Act.

Users should always be informed about what gaze data is collected, how it is processed, and who has access to it, particularly for uses involving advertising or automated decision-making. Transparency is paramount, and it is the cornerstone upon which trust is built between technology providers and users.

The Necessity for Privacy By Design

In this context, the concept of privacy by design becomes critical. This approach advocates for privacy to be a core consideration throughout the development process of new technologies, not an afterthought. For gaze tracking, this could mean default settings that favor less collection of personal information, straightforward options for disabling data collection, data minimization practices such as limits on retentions and de-identifying or anonymizing data whenever possible, and implementing security measures, specifically when gaze data is transferred off device or to external parties.

Responsible Artificial Intelligence Considerations

In addition to privacy considerations, companies that collect gaze data should be aware that regulators are taking note of the impact that collecting personal information, particularly sensitive personal information, can have in delivering artificial intelligence (AI) tools. For example, a number of state privacy laws in the United States

impose additional obligations on use of personal data in automated decision-making, especially for decisions that produce a legal or similarly significant effect on or result in profiling of the individual. These obligations generally include performing a risk assessment and providing additional notice and the opportunity to opt out of such processing.

The FTC has also weighed in on tracking individuals' movements using biometric data, particularly in ways that they may not be aware of. In its Biometric Policy Statement, the FTC expresses that engaging in "surreptitious and unexpected collection or use of biometric information" may be "unfair in and of itself," especially when performed "in a manner that exposes the consumer to risks such as stalking, exposure to stigma, reputational harm, or extreme emotional distress." Soon after publishing its Biometric Policy Statement, the FTC brought its first enforcement action alleging that discriminatory use of AI was an unfair practice under Section 5 of the FTC Act. The complaint was brought against retail pharmacy Rite Aid for its use of facial recognition technology as an anti-shoplifting and security tool. In part, the complaint alleged that failing to implement reasonable safeguards to prevent false positives was an unfair practice. While the FTC did not address gaze data specifically, companies that use gaze data, specifically for monitoring purposes, should take note that regulators likely expect transparency regarding use and rigorous review before relying on automated systems to make decisions that are likely to result in substantial injury to consumers.

The White House has also referred to the potential of gaze data specifically. In its 2023 AI Executive Order, the White House calls for the need to examine use of "gaze direction" and "eye tracking" when encouraging the Architectural and Transportation Barriers Compliance Board to ensure that people with disabilities benefit from AI while being protected from its risks.

As gaze tracking technology becomes more sophisticated and widespread, ethical considerations must guide its implementation.

As we continue to integrate technology into every facet of our lives, gaze tracking can be a powerful way to enhance immersive experiences, obtain valuable insights, and enable new forms of interaction—but it is not without its obligations and risks. Companies using gaze tracking need to carefully balance the benefits of delivering personalized experiences with the obligations and responsibilities of protecting user privacy and complying with applicable legal frameworks. Striking the right balance can be challenging, particularly with an ever-evolving legal landscape. Working with knowledgeable privacy and regulatory counsel can guide companies to develop and deploy gaze tracking technologies in a manner that is compliant and builds trust and loyalty with customers.

**The authors would like to acknowledge Irena Cronin, CEO & Founder of Infinite Retina for their contributions to this blog post.*

Follow us on social media @PerkinsCoieLLP, and if you have any questions or comments, please contact us here. We invite you to learn more about our Digital Media & Entertainment, Gaming & Sports industry group and check out our podcast: *Innovation Unlocked: The Future of Entertainment*.

Authors

Jason Schneiderman

Partner
JSchneiderman@perkinscoie.com 650.838.4333

Bipasana Sakya Joshee

Counsel
BJoshee@perkinscoie.com 206.359.3285

Explore more in

Technology Transactions & Privacy Law
Blog series

Age of Disruption

We live in a disruptive age, with ever-accelerating advances in technology largely fueling the disruption permeating almost every aspect of our lives.

We created the *Age of Disruption* blog with the goal of exploring the emerging technologies reshaping society and the business and legal considerations that they raise. Subscribe ?

View the blog