**Interviewer:** Could you please introduce yourself a little bit?

**Researcher:** My name is “Researcher”. I'm a professor at “University A” and my research is in machine learning, particularly within what I call AI information. This involves information we can measure and obtain from mostly human eyes. I've been doing this for many years, developing AI trackers and methods for analyzing data and inferring information about humans primarily from eyes, though I also work on other things.

**Interviewer:** How do eye-based biometrics compare to traditional methods like fingerprints or facial recognition in terms of security and resistance to spoofing?

**Researcher:** There are very significant and important differences. You can identify a human being from multiple factors—many more than people actually think. Iris recognition is well known, but what's less recognized is that the way you move your eyes when exposed to certain stimuli also reveals who you are, and you can't control it by any means.

With facial recognition or fingerprints, you can potentially alter them, but you can't do that with things happening in your brain that are reflected in your eye movements. This makes a profound difference in the amount and reliability of information you can obtain.

Iris recognition is very well established and scales effectively. What people often don't realize is that eye movements reveal a tremendous amount about you—your interests, identity, activities, and various aspects of cognition. Since most people don't understand this, they don't know what they're consenting to when their eye data is collected.

**Interviewer:** Can gaze patterns be used for continuous identification? How does this improve security over one-time authentication methods?

**Researcher:** Yes, it has been done. How well it compares to other methods is another question, but it can definitely be used for identification. It can also be used for entering passwords. The iris pattern essentially defines who you are, while your gaze patterns could reveal a password. Some patterns are more reliable than others. For example, writing your own name with your eyes.

[Brief personal exchange about the interviewer's background]

So yes, you can extract both password information and identity from eye data.

**Interviewer:** How do you address potential attacks, such as replay attacks or deepfake-based spoofing on gaze tracking authentication systems?

**Researcher:** That's an interesting question. I haven't seen many people working with generative models for eye data. My claim—and please don't publish this as I'm writing something about it currently—is that eye information is governed by a triangle: who you are, what you're doing, and where you're doing it. These parameters govern your eye movements.

Not all parameters might be present for all kinds of tasks, persons, or contexts. For example, your eye movements while driving might resemble those while riding a bike or running. There's overlap, which is why I'm reluctant to make definitive claims about spoof attacks.

You can spoof iris recognition patterns—that's been demonstrated. The question is whether they resemble patterns already in your database. Most authentication systems use additional parameters like detecting heat around the face. A screen generating a pattern won't generate the right heat signature.

Systems also check if eye movements appear natural. But generally, with advanced generative models that truly model the underlying distribution—don't quote me on this—you're in trouble. How can a system distinguish these things unless you have some other verification parameters?

**Interviewer:** Are there any known adversarial attacks that can trick eye tracking-based biometric systems? If so, how can they be mitigated?

**Researcher:** As I just mentioned, if you generate an iris pattern that looks like a legitimate user's eyes, you can try to log into the system. If you can also generate convincing live sequences with heat signatures and natural movements that circumvent security measures—well, as Carlsen Sherman says, no digital system is completely safe. This would be an example of that vulnerability.

**Interviewer:** Since gaze can reveal personal and psychological traits, what are the main privacy risks associated with continuous eye tracking?

**Researcher:** There are many risks. I think the biggest issue right now is that we don't fully understand eye tracking as a signal. We can't properly assess the real risks. When someone moves their eyes, sometimes we can distinguish individuals and reveal traits about reading efficiency or attention patterns, but we're never 100% certain because there are multiple possible interpretations.

However, this doesn't mean eye tracking doesn't provide valuable information. Just like the governor's example—when you combine eye data with other information, you suddenly know much more. The problem is that you're getting more than just one bit of information, and this enables profiling.

When companies like Meta collect your eye data through virtual and extended reality headsets, they combine it with other data to create much finer, detailed profiles of individuals. Most people aren't aware of this, and there's little they can do about it. People don't know all the information their iris patterns might reveal, and honestly, nobody fully does because we don't know with what accuracy we gain this information.

**Interviewer:** How can users be assured that their eye movement data is not being misused for surveillance or tracking beyond identification purposes?

**Researcher:** I don't think they can be assured. If they're not aware of what's happening, they can't control it. Standard cameras can measure some eye movements, but their resolution is limited. Some details require pupil imagery, which captures changes in the pupil. However, most of these changes are due to light conditions, making it difficult to filter out environmental noise when measuring in real-world settings.

The fundamental problem is that nobody knows exactly how much information is revealed through eye tracking and with what accuracy. This is essentially unknown.

**Interviewer:** What security measures should be taken to protect stored eye tracking data from leaks or unauthorized access?

**Researcher:** My PhD student is actually looking at this right now. You can essentially use standard security practices—ensuring data isn't revealed to unauthorized parties, storing it securely with password protection, encryption, and so on. These measures apply to eye tracking data just as they would to any sensitive information.

The problem is context. If I give you just an iris pattern, you don't know who the person is or what task they were performing. What would you use it for? You might be able to identify someone based on their eye movements, but most likely not without knowing what they were doing, where, and under which conditions.

The problem becomes more significant with extended reality headsets, where you're in a more constrained environment with more detailed information collection. If someone hacks into VR headsets and obtains the image data, they could develop generative models of people's eyes and their movements. That's clearly a security risk.

**Interviewer:** Could gaze tracking data be used to infer a user's cognitive state or emotions in ways that might pose ethical dilemmas?

**Researcher:** Yes, clearly. I used this example in my inaugural lecture when I became a professor. I mentioned a company (I think it was Netflix) where it was considered sexual harassment to look at another person for more than 10 seconds. Now we have a way of measuring this directly.

The problem is that just because my eyes are pointing toward you doesn't mean I'm actually paying attention to you. Students might be staring at the blackboard during my lectures but mentally be somewhere else. We can't measure this solely from eye information.

But yes, there are many things you can infer—reading proficiency, attention to details, observation patterns, preferences including sexual preferences, and more. This is how you obtain information about people—by observing what they look at. Some eye movements are subconscious and some are voluntary, but for short periods, you have no control over these movements, which reveals a lot about you.

People study these personal traits, micro-gestures that can't be controlled, and sometimes that one bit of information is enough to make significant inferences.

**Interviewer:** How could eye tracking be used in high-security environments like financial transactions or border control?

**Researcher:** It's just another metric you can use for identification. You can verify that the iris pattern matches the person, that the visual password is correct, and that characteristics like the maximal velocity of eye movements (governed by muscles in the eyes) are correct.

There are many possibilities because it's biometric. The eye is controlled by muscles and is essentially the only visible part of the brain—it's directly connected to your brain. Emotions are also reflected in eye movements, so you have some certainty about who the individual is.

But nothing is perfect. With good generative models, you can model anything, including heat signatures and other factors. If you can do that, you can potentially fool any system.

**Interviewer:** Are there any specific cryptographic techniques that can be applied to protect eye tracking data while maintaining usability?

**Researcher:** Sure, if you can encode and decode quickly, there's no problem.

[Brief exchange about interviewer's supervisor]

You could use cryptographic protocols if they're real-time or whatever you need. It's just encryption of data. The question is, if you have high-quality eye trackers capturing 1000 frames per second over extended periods and need to transmit this over a network, then you face bandwidth challenges.

Another issue is that when you train a machine learning model, the original data essentially disappears. My PhD student David is looking at how, even with a trained model, you can verify that the model comes from a specific dataset. That's proving to be a difficult problem to solve.

**Interviewer:** Can gaze tracking be integrated with blockchain or zero-knowledge proofs for privacy-preserving authentication?

**Researcher:** Perhaps, I don't know. I haven't looked enough into these technologies.

**Interviewer:** How do legal and regulatory frameworks such as GDPR impact the development of secure and privacy-preserving eye tracking applications?

**Researcher:** All our information is governed by GDPR. Everything you do needs to consider what happens with the data and how it's used. Eye tracking data is like fingerprint information times ten in terms of sensitivity.

So regulations have impacted development significantly, and many people are focusing on privacy within eye information. The biggest problem, though, is that many of the methods claiming to protect privacy don't actually work. That's a huge issue. My PhD student David is working on a review paper about these challenges. What people think is secure is often not secure at all. Essentially, we're close to the Wild West in terms of regulation effectiveness.

**Interviewer:** Could eye tracking be used as a multi-factor authentication component alongside other biometrics or behavioral traits?

**Researcher:** Absolutely, 100%. If you combine fingerprints, eye tracking, facial recognition, hair growth patterns, and other biometrics—yes, certainly.

**Interviewer:** How do you see the future of eye tracking technology evolving as a secure biometric modality in the next decade?

**Researcher:** I'm 100% sure that it will continue developing. I have colleagues working with Meta, for example, on privacy and security aspects. It must be integrated into products, and developers need to ensure compliance with European legislation when creating tools like Meta's headsets.

I think we need a couple more years before these technologies are fully mature for commercial deployment. You can apply whatever existing encryption technologies you have, but I think there are many more ethical questions that need to be addressed.

**Interviewer:** I don't have any more questions.

**Researcher:** Okay, that was simple.