TECHNEWSWORLD™

Report Finds Biometric Data Threatened by Social Media

John P. Mello Jr.

October 19, 2022

Sharing high-resolution media online can unintentionally expose sensitive biometric data, according to a report released Tuesday by a cybersecurity company.

That can be particularly dangerous, the 75-page report by Trend Micro noted, because people don't know that they're exposing the information.

The report cited, as an example, the #EyeMakeup hashtag on Instagram, which has nearly 10 million posts, and #EyeChallenge on TikTok, with more than two billion views, exposing iris patterns good enough to pass iris scanners.

"By publicly sharing certain kinds of content on social media, we give malicious actors the opportunity to source our biometrics," the report explained. "By posting our voice messages, we expose voice patterns. By posting photo and video content, we expose our faces, retina, iris, ear shape patterns, and in some cases, palms and fingerprints."

"Since such data could be publicly available, we have limited control over its distribution," it added. "We therefore don't know who has already accessed the data, nor do we know for how long the data will be retained or for what purposes."

Not a Panacea

The report covers what kinds of biometric data can be exposed on social media and outlines more than two dozen attack scenarios.

“The report illustrates that biometric identification is not a panacea,” observed Will Duffield, a policy analyst with the Cato Institute, a Washington, D.C. think tank.

“As we design identification systems, we need to be aware of technologies coming down the pike and potential misuses in the real world,” he told TechNewsWorld.

“Trend Micro raises some valid concerns, but these concerns are not new to biometrics professionals,” Sami Elhini, a biometrics specialist with Contrast Security, a maker of self-protecting software solutions in Los Altos, Calif., told TechNewsWorld.

He noted that there are various ways to attack biometric systems, including the “presentation” attacks described by the report, which substitutes a photo or other object for a biometric element.

To counter that, he continued, “liveness” must be determined to make sure the presented biometric is that of a live person and not a “replay” of a previously captured biometric.

Avi Turgeman, CEO and co-founder of IronVest, an account and identity security company in New York City, agreed that “liveness” is a key to foiling attacks on biometric protections.

“The Trend Micro report raises concerns about fraudulent biometrics created through social media content,” he told TechNewsWorld. “The real secret in fraud-proof biometrics is liveness detection, something which can’t be recreated through pictures and videos collected on social media.”

One Factor Not Enough

Even when testing for liveness, biometrics can still be too easy to bypass, maintained Erich Kron, security awareness advocate for KnowBe4, a security awareness training provider in Clearwater, Fla.

“Holding a phone in front of a person’s face while they sleep can unlock the device, especially when they use it with the default settings, and gathering fingerprints is not a difficult task,” he told TechNewsWorld.

“Even more concerning is that once a biometric factor is compromised, it can’t be changed like a password can,” he added. “You cannot change your fingerprints or facial structure in a long-term way if breached.”

If the Trend Micro report illustrates anything, it’s that multi-factor authentication is a necessity, even if one of those factors is biometric.

“When used as a single factor for authentication, it’s important to note that biometrics can be subject to failure or manipulation by a malicious user, particularly when that biometric data is publicly available on social media,” said Darren Guccione, CEO of Keeper Security, a password management and online storage company based in Chicago.

“As the capabilities of malicious actors to take over accounts using voice or facial biometric authentication continue to grow, it is imperative that all users implement multiple factors of authentication and strong, unique passwords across their accounts to limit the blast radius if one authentication method is breached,” he told TechNewsWorld.

Metaverse Problems

“I don’t like to put all my eggs in one basket,” added Trend Micro Vice President of Infrastructure Strategies Bill Malik. “Biometric is good and useful, but having an additional factor of authentication gives me much more confidence.”

“For most applications, a biometric and a PIN are fine,” he told TechNewsWorld. “When a biometric is used alone, it’s really easy to forge.”

Collection of biometric data will become even more of a problem when the metaversebecomes more popular, he asserted.

“When you get into the metaverse, it’s going to get worse,” he said. “You’re putting on these $1500 goggles that are tuned to not only give you a realistic view of the world but are constantly monitoring your micro-expressions to figure out what you like and don’t like about the world that you’re seeing.”

However, he's not worried about that additional biometric data being used by digital desperadoes to create deepfake clones. "Hackers are lazy, and they get just about everything they need with simple phishing attacks," he declared. "So they're not going to spend a lot of money for a supercomputer so they can clone somebody."

Device-Tied Biometrics

Another way to secure biometric authentication is to tie it to a piece of hardware. With the biometric enrolled on a specific device, it can only be used with that device to authenticate the user.

"This is how Apple and Google's biometric products today work — it's not just the biometric that's being checked when you use Face ID," said Reed McGinley-Stempel, co-founder and CEO of Stytch, a passwordless authentication company in San Francisco.

"When you actually perform a Face ID check on your iPhone, it's checking that the current biometric check matches the biometric enrollment that's stored in the secure enclave of your device," he told TechNewsWorld.

"In this model," he continued, "the threat of someone being able to access photos of you or having your fingerprint does not help them unless they also have control of your physical device, which is a very steep hill to climb for attackers given the remote nature in which cyber attackers operate."

Losing Control of Our Data

As users, we are losing control of our data and its future uses, and the risks from the platforms we use every day are not understood well by the common user, the Trend Micro report noted.

Data from social media networks are already being used by governments and even startups to extract biometrics and build identification models for surveillance cameras, it continued.

The fact that our biometric data cannot be changed means that in the future, having such a treasure trove of data will be increasingly useful for criminals, it added.

Whether that future is five or 20 years ahead, the data is available now, it stated. We owe it to our future selves to take precautions today to protect ourselves in the world of tomorrow.