With the Proliferation of Biometric Scanning, Some Hidden Risks

In today's digital world, few words are as dreaded as "hacked." What started in the 1960s and 70s as an often-mischievous attempt by young coders to outwit the cutting-edge technology of their time has become an urgent matter of personal and national security as more and more data is stored on our devices.

Researchers have found a way to simulate fingerprints and fool scanners as much as 20 percent of the time.

Cybersecurity experts have tried to curtail data theft in recent years through biometric scanning, in which an individual's face, iris, or fingerprint are used as a key to access personal data. Commercial biometric technology was popularized in 2013, when Apple included a fingerprint scanner on the iPhone 5S, and since then technology companies like Google, Samsung, and Huawei have followed suit, rolling out devices with facial recognition as well.

And yet, even these advances have become vulnerable to sophisticated hacking techniques. A team of researchers at New York University's Tandon School of Engineering, for instance, created an algorithm to not only simulate a person's fingerprint but to create a single print that can masquerade as several others and fool scanners as often as 20 percent of the time — all without replicating an actual print.

So much for the peace of mind that biometric scanning once promised. Indeed, as biometric security technology increasingly saturates our digital lives, a growing number of experts are expressing concern that the consequences of a security failure — a practical inevitability, they say — are only getting higher. "You can always replace your credit card, but you can never replace your fingerprint or iris," says Kon Leong, CEO and co-founder of the data archiving company ZL Technologies, "This means that any breach would require an overhaul of the entire infrastructure. Furthermore, it is not a matter of *if* there will be a breach. It is a matter of *when*."

And as the tug-of-war between hackers and security experts escalates, the implications for individual consumers and citizens — who are drafted into each new iteration of these technologies at airports, borders, and banks, and on their smartphones, tablets, and computers — become increasingly complex.

"Data can be linked and connected to track individuals or produce personal profiles unprecedented in detail, availability, and durability," the editors Irma van der Ploeg and

Jason Pridmore write in the introduction to their 2015 book “Digitizing Identities.” “Once registered, such attributes are virtually impossible to erase.

“One’s digital identity, or digital persona,” they added, “can cast long shadows over one’s life.”

Much like a master key can fit many different locks, the NYU Tandon algorithm, called DeepMasterPrints, focuses on generating artificial prints that contain *enough* common fingerprint characteristics to allow them to fool fingerprint sensors into believing they’re a match. In order to do this, researchers use a three-step process.

Hackers can use 3D printers to generate images of prints that can be transferred to wearable, thimble-like devices.

“The first step is just learning what fingerprints are,” says Philip Bontrager, a Ph.D. candidate who co-authored a paper on the technology. After analyzing fingerprint databases to learn the basic structure of a print, the algorithm generates possible master prints and evaluates those to pinpoint which ones have the best shot at fooling a scanner. Testing those prints on low, medium, and high levels of sensor security, the research team found that DeepMasterPrints fooled commercial fingerprint verifiers roughly one out of five times when tested against mid-level security.

Arun Ross, a professor in the Department of Computer Science and Engineering at Michigan State University and another co-author on the paper says the relatively low security threshold of handheld devices like smartphones makes them particularly vulnerable. Their sensors create a user profile that accepts several partial matches for a fingerprint instead of a single exact match, in part because the sensors are too small to discern a full print.

Ross and Bontrager say that while users don’t need to start panicking yet, hackers with access to 3D printers, which are becoming increasingly common, could theoretically generate images of prints that could be transferred to a wearable, thimble-like device to unlock phones left in public places like library desks or coffee shops.

At the Idiap Research Institute in Switzerland, researchers are also working to expose the vulnerabilities of biometric systems. Sébastien Marcel, head of the Biometrics Security and Privacy group at Idiap, says that while fingerprint scanners may be an easy target because of their prevalence, systems that rely on facial or iris recognition are not necessarily more secure, especially with the spread of personal photos on social media.

Marcel says researchers have been working with technology companies to help them identify and strengthen their security through anti-hacking techniques like incorporating more fool-proof data (e.g. temperature, blood flow detection) into their identification criteria.

Both Marcel and the NYU researchers agree that two-factor identification can be a practical solution, whether it be two forms of biometric identification or a biometric and a pin code. But even this could be hackable, Marcel cautions.

Instead, he urges greater transparency among researchers, businesses and the public. "I'm not convinced that by hiding things we improve the security," says Marcel. He thinks that, to some extent, security is best "if we share and inform about the vulnerabilities" that are discovered.

Other researchers are concerned about the social consequences of biometrics. In a 2008 paper titled "Body, Biometrics and Identity," the Italian researcher and psychoanalyst Emilio Mordini and his co-author Sonia Massari cited two main concerns about the future of biometrics.

"You can always replace your credit card but you can never replace your fingerprint or iris."

The first is "function creep," or the extra data a biometric scanner might gather without users' explicit consent, such as information about skin color, age, and even perceived emotion. The authors warned that increased use of biometrics could result in a massive amount of "shadow" data that could potentially be used to profile or discriminate, and thus has "the potential to erode public trust and destroy confidence in a given system."

The second concern is what the authors refer to as the "digitization" of the body. They argue that when something as complex as a human being is simplified to its numerical components (e.g. facial structure, voice signature etc.), one can feel a sense of disembodiment, as if inhabiting one's body instead of *being* it. The authors write that this has led philosophers to consider the potential loss of "human essence" and ultimately human dignity as a result of digitization.

In the end, though, it could be that the risks that come with biometric hacking are worth taking after all. "If the war between privacy and exposure is winnable, then we either live in fear of our neighbors, or we live under big brother," says Leong. "Therefore, it's in our best interest that the war between privacy and exposure remains unwinnable."