5 Ways Biometric Security Can Be Spoofed

5 Ways Biometric Security Can Be Spoofed

by **James Corbett**, *The Corbett Report*
February 13, 2021

Remember when you were a kid and you tried to imagine what the world was going to look like in the far off, sci-fi sounding year of 2021? What did you imagine? Weekend holidays to the moon? Flying cars and jetpacks to take you around the elevated cities? Robot butlers? The end of all diseases? Star Trek-style replicators and holodecks?

Well, snap out of it, kid. This is what 2021 really looks like:

Sheeple lines up for the slaughter. Colourized. 2021.

In case you didn't know, that's the handy-dandy contactless facial recognition gate from NEC. Yes, you don't have to worry about fiddling with your mask to allow your algorithmic overlord to scan your face and allow you entry to a building, terminal or security perimeter anymore! Thanks to the good folks at NEC, you can now maintain your social distancing and be electronically tracked and herded like the pliable tax cattle you are without even taking your mask off!

"But what about those poor souls living in third world nations?" I hear you asking. Never fear! Thanks to the non-profit Simprints Technology (in partnership with Gavi, the Bill & Melinda Gates Foundation, USAid and other benevolent philanthropic institutions), there are contactless biometric scanners for them, too! Simprints' biometric solution allows governments to more effectively tag and track their human property, issue them an electronic brand, and make sure they get processed through the system all without having to come within six feet of another human being!

And just in case you're upset that you're missing out on the fun, you can rest assured that some version of biometric ID is going to be rolled out in your local area in the very near future . . . all to keep you safe from the deadly bogeyvirus, of course. (Did someone say COVID passport?)

But there's just one little thing to consider in this headlong rush to get the entirety of the human species' biometric details entered into the computer matrix: biometric systems are notoriously buggy, hackable and open to spoofing. But why let a little identity theft get in the way of the New Biometric Normal, eh?

Still, for those who insist, here's a break down of just five of the ways that this biometric scanning technology can be hacked, gamed, spoofed or tricked.

1. Forging Fingerprints

Your fingerprint. As unique as a snowflake, those swirls and whorls on the ends of your fingerprints are—as we all know from any number of detective stories or crime procedurals—perfect for identifying you at the scene of a crime. But before they became a staple piece of evidence for the Scotland Yard types, the study of fingerprints was systematized by Charles Galton, the father of eugenics.

It should hardly be surprising then, that fingerprints were the first thing that the boffins turned to in their quest to create a biometric identification system. In 2021, we are already well past the point where fingerprint scanning is considered some sort of futuristic, sci-fi way of gaining access to a system. Indeed, with the advent of TouchID many people around the world now use their fingerprint as their password as a matter of course.

But as long as there have been fingerprint ID systems, there have been warnings that such systems are easily spoofed.

Like in 2002, when Japanese researchers used gummy bear gelatine to mould fake fingers that could fool fingerprint detectors 80% of the time.

By 2005, researchers in the US had increased that false fingerprint verification rate to 90% using dental materials, Play-Doh and severed cadaver fingers.

Think the fingerprint scanner makers could make an easy work around to such crude spoofs? Think again. In 2016, a journalist was able to use the same dental mold and Play-Doh trick to hack into an iPhone in five minutes. In fact, he assures us it would've taken even less time if he had had a public photo of the hand in question. That's no exaggeration, either. In 2014 a hacker used a photo taken of German defense minister Ursula von der Leyen at a press conference to clone her fingerprint.

Still think fingerprint identification is a good idea? Ok, how

about facial recognition . . .

2. Faking Faces

Using a face scan to "unlock" a digital system may sound just as plausible as using a fingerprint. After all, everyone has a unique face, right?

Well, no. Actually, even a second's thought might bring up some interesting exceptions to that rule. What about idential twins? Surely the identical twin of a facial ID system's user could fool that system into granting the twin access, right? As it turns out, yes, most of the time twins can fool the system. But in a strange way it brings even less comfort to know that sometimes (but only sometimes) the twins *can't* gain access to each other's devices with their identical faces.

But if you think *that's* bad, get a load of *this*. In 2017, Apple refunded one Chinese woman's iPhoneX purchase when it was found that her coworker (*not* her identical twin) could unlock her phone with *her* (the coworker's) face. This may be part of the well-documented phenomenon that facial recognition technologies have a harder time distinguishing non-white faces, leading to many false verifications.

Of course, it's not just poor recognition algorithms that one has to worry about with facial recognition. Just like with forged fingerprints, hackers have found ways to fool face scanners into approving access for fake faces. One demonstration of this involved cybersecurity firm Bkav showing that they could fool the iPhone's FaceID system with a $150 mask made with a combination of 3D printing, a silicone nose and printed images of the eyes.

3. Imitating Irises

OK, what about iris scans? You've seen it used in a million pieces of sci-fi predictive programming over the years. The scientist steps up to the locked door of the high-tech

laboratory, a beam of light scans his eyeball, and *voila*! The door is open.

Yeah, that's a bunch of hooey, too.

Less than a month after Samsung launched its Galaxy 8 smartphone hackers had already figured out how to foil its iris recognition feature using nothing more than a camera, a laser printer and a contact lens. Still, the fact that the feature even lasted a month before it was broken might be to its credit; the facial recognition feature was defeated before the phones even shipped using nothing more than a picture of the owner's face.

4. Hacking Hashes

But what about those lazy hackers out there? What if you just don't want to go through the rigamarole of creating fake fingerprints or imitation irises? Or what if you're just out of Play-Doh and Gummy Bears? Don't worry, there's an easier way: hacking.

Why bother trying to fool the scanner when you can just hack into it? And if you can hack into a biometric database then you can acquire not just one set of biometric credentials, but millions. Or billions.

Think that's an exaggeration? Just look at Aadhaar. As you know by now, Aadhaar is the world's largest biometric identification scheme, having collected a digital photograph, ten fingerprints, and iris scans of over one billion Indians in the past several years. As you also know, it enjoys the vocal support of Bill Gates (of course) and was pioneered by Gates' friend, philanthropic partner and "hero," Nandan Nilekani.

What you may not know is that the software used to enroll new users into the Aadhaar database was compromised years ago. A software patch that was available for purchase for 2,500

Indian rupees (about $34) could override the system's security features, allowing unauthorized users to add accounts for anyone, generating unique identification numbers that could then be used to access Indian government services. As the more in-depth reports on the hacks elaborated, it was being widely used by operators to increase their margins on enrolling new users by allowing them to log in to several machines simultaneously.

The Unique Identification Authority of India (UIDAI) which operates the Aadhaar scheme was quick to downplay reports that anyone's biometric details had been compromised. The patch only allowed hackers to add accounts, not read accounts. See? Nothing to worry about!

Continue giving your fingerprints with your tax returns. Have your 12-digit biometrically-issued ID number ready when you get your vaccine. Open your eyes nice and wide for the iris scan before you get your government rations. I mean, it's not like your personal details could ever be breached by a biometric database hack, right?

5. Bypassing Biometrics

Yes, you *could* go to great lengths to construct fake fingerprints or irises or other elaborate ruses to fool the biometric scanners. Or you *could* try to hack into the biometric databases themselves to steal people's identity. But there's an even more direct route for the would-be hacker who is a little lazy: routing around the scanner altogether.

In a lame attempt to downplay the iris scanner hack referred to in section 3 above, Securlinx ends up making a good point: it's much easier to bypass a system than it is to enact an elaborate scheme for tricking a scanner.

Why not just blow away the whole database of iris templates? Problem solved. The scanners, now just locks with no key, would have to be disabled at least temporarily.

If stealth is more your style, just hack into the database, create a credential for yourself by placing your very own iris template in there and dispense with the whole rigmarole of the hill-climbing business. Delete your template (and why not all the others) after the heist.

[. . .]

You could trick, threaten or bribe someone into letting you in.

Break the door or a window.

They're not wrong. Getting into a system can sometimes be a lot easier than the elaborate Mission Impossible-style spy stuff outlined above. After all, we're told it was a simple phishing attempt that got Podesta's emails. Sometimes all you need to rely on is the stupidity of the average person.

Conclusion

Yes, biometric systems are notoriously hackable, spoofable and breachable. And the worst part is that, unlike a run-of-the-mill password, once your face or iris or fingerprints get hacked there's nothing you can ever do to change them.

But in pointing out the inherent lack of security in these biometric systems, we run the risk of falling into a trap. We might be seen to be implicitly stating that if these security loopholes could be closed then biometric identification would be a good thing. But that is not the point.

These systems are being put into place to tag, track and database the human population just like a rancher keeps tabs on his cattle, and for much the same reason. To the politicians who administer system for the technocrats who manage the system for the banksters who create the system, we are merely tax cattle to be penned, herded, fattened, sheared, and, when need be, slaughtered. The biometric ID is just a more efficient way to facilitate that purpose.

It starts off small. It's just a TouchID scanner on your "smart"phone. It's just a fingerprint for your passport. It's just a face scan at the airport. It's just a digital photo for your Real ID. It's just a biometric scan to pay for your groceries. . . . Once the countours of the biometric prison planet come into view, it's already too late. The bars have been slammed shut and the door locked.

But don't worry. If you get your biometric driver's license and government ID and tie it into your vaccination record and social credit score then maybe they'll let you have your dream of flying cars after all.

To the future!

*This weekly editorial is part of **The Corbett Report Subscriber** newsletter.*

To support The Corbett Report and to access the full newsletter, please sign up to become a member of The Corbett Report website.

cover image credit Tumisu / pixabay