Evading the Misuse of Biometric Data

We understand that the Taliban is now likely to have access to various biometric databases and equipment in Afghanistan, including some left behind by coalition military forces. This technology is likely to include access to a database with fingerprints and iris scans, and include facial recognition technology. Overall, it is very difficult to avoid recognition based on biometric data, but here are some things you can do, and some you shouldn't.

FACIAL RECOGNITION

Just a couple of frames that your face appears on in an active surveillance camera can be used to identify you.

The best way to bypass facial recognition is to look down, and stay looking down. If you are on a camera of any sort, that camera footage could at any time be run for facial recognition. By looking down, a side or front-on face profile is most easily avoided by even the most high end equipment.

You want to obscure or alter as many major facial structural features as possible, most importantly the mouth, nose, eyes, jawline, and cheekbones below your eyes. Doing this means adding things that can change their shape, or wearing things that obscure them, or a combination of both. Hide as many of these features as you can - each alteration lowers the chance that you are identified, but cannot guarantee you won't be.

But bypassing an individual supervised facial recognition test, such as at a security station, is extremely unlikely. In a real emergency, try distorting your facial structure as much as you feel you can get away with, using mainly your cheek and forehead muscles.

While probably too difficult for most people, it's possible to apply so many layers of makeup it can appear to change the structure, not just the color, of your face, and give you a chance at not being identified. A useful guide is looking into SFX Makeup Prosthetics such as (https://www.instructables.com/How-to-Make-SFX-Makeup-Prosthetics/). If you do not have access to plaster or latex, you can experiment with different materials that stick to your face and hide with makeup. Remember to change more than just one part of your facial structure.

You can test this on a smartphone's Face ID, which uses fairly primitive technology. But if you can't fool your smartphone, you probably won't be able to fool the higher tech facial recognition technology.

It's possible to obscure your face with long hair, but it's generally not useful to change your glasses, makeup and facial hair as facial recognition technology reads facial structure. You might fool humans that way (which could also be useful), but not the tech.

FINGERPRINT SCANS

Fingerprint scans are difficult to bypass. There are four types of scans. Some also include prints below your first joint, multiple fingers, and the sides of your fingers, and all may be tested. If they are using a wireless handheld device, it most likely will be fingerprint or palm.

While It's possible to create a fake print to glue to your finger, this is highly risky and should only be considered in an emergency. Your fingers may be put through a close visual examination before the test and fake prints are easily identified during this process. Again, you can test this on your smartphone fingerprint scanner, but this is likely to be lower tech than the best scanners.

For more info on this difficult operation see https://www.wikihow.com/Fake-Fingerprints.

Burning or otherwise mutilating your fingertips will stop the tech from recognising you, but it obviously raises suspicions. Cutting your fingertip is unlikely to remove enough of the print to be detectable.

In an emergency the best thing you can do is try to stop the scanner giving a good read.
If you are elderly you have deeper fingerprint ridges, and pressing down hard, or leaning your finger to one side or the other might smudge the print enough to fool the tech. If your hands are very dry or dirty this can also cause a failure to read.

IRIS SCANS

Iris scan recognition tests are extremely accurate and difficult to bypass if administered with proper equipment. The iris scanners read unique patterns in the colored circles in your eyes.

Successfully evading these scans is very unlikely, but there are a couple of things you can try.

1. Use colored contact lenses. This might work if a light is not shone directly into your eye during the test.
2. Using a drug, e.g. Tropicamide, to dilate your pupils. Tests suggest this works in about one in ten cases, and involves taking drugs that could alter your mental state.

3. Shake or move your head. This can prevent the test from running. Shaking or moving your head in rapid small movements can prevent the sensitive test from successfully running. This only has a chance of success against low tech equipment.