6 Ways To Defeat Facial Recognition Cameras

Would you like the ability to control when your image is or is not captured by facial recognition software?

Many Americans feel abuse of this technology routinely violates either the God-given or constitutional rights of US citizens.

Facial recognition software enables the image of a subject to be identified by assigning values for the relative proportions of aspects of the subject's face, and then comparing to databases of values for the faces of individuals whose identity is known, such as databases of passports, military ID's, driver's licenses, law enforcement databases, year books, school records and so on.

Newer technologies employ three-dimensional information about the shape of a face and skin texture analysis. This information can be misused to violate rights such as freedom of assembly, freedom of movement and, some believe, can constitute unlawful search and seizure or other rights violations.

Rights and Property Predate Law

Law was created in order to protect rights and property, but is now all too often used to legally plunder them.

Professor Alessandro Acquisti conducted a series of experiments at Carnegie Mellon University (CMU) which identified strangers, identified their personal information and, in some cases, even social security numbers and credit reports. The experiments were both on-line and off-line and used only photos, social media and resources available to end

users.

He demonstrated the ability at the BlackHat security conference in Las Vegas … five years ago in 2011!

Think this technology is only available to the government and highly paid private investigators? Unfortunately, it's attainable by pretty much anyone who knows how to read and has the will and a smartphone. CMU even developed an app that overlays personal information on an image of the person's face.

I don't think the fact that facial recognition software and social media increase privacy risks is a new idea to most people, but I think that the seriousness of their personal exposure often is. People tell me all the time that they don't like to think about privacy, and global surveys bear out the fact that people tend to ignore known cybersecurity risks the world over.

Does your own normalcy bias extend to social media?

Is privacy a factor when you choose smartphone apps?

Do you manage your on-line data footprint?

How easy would it be to identify you using facial recognition?

I'm not talking about the government, police or tech nerds wearing products like Google Glass here. I'm talking about anybody with the will and a smartphone being able to not only identify you, but access your personal or sensitive information.

I'm sure most of you do not lay awake nights worrying about whether it is possible to identify you through facial recognition, but could you successfully avoid facial recognition if you determined you had a need to do so?

Many preppers find it useful to consider "what if" scenarios

involving grid-down, WROL (Without Rule of Law) scenarios in the theoretical vacuum of a technology-free world. Placing theoretical boundaries on survival scenarios is fine for recreational daydreaming, but less effective as an aid to serious preparation. With the sheer number of cameras in circulation, some will likely still be working in the majority of scenarios.

A reversible hat, two or more hats of different colors and designs may enable you to quickly change your appearance enough to escape detection by someone with a verbal description of you.

Hats, long-sleeved shirts, hoodies, reversible jackets, sunglasses, umbrellas, newspapers and gloves are all tools that aid in masking physical characteristics, enabling you to stand out less if you have to travel through, as area where you may be perceived as an outsider or wish to remain anonymous, on or off camera.

1. Camera Finders

Cameras can sometimes be detected and avoided if you see them before they see you, or if you know where they are ahead of time. Then they can be neutralized with something as simple as a disguise, a tilt of the head or placement of an opaque object between you and the camera you wish to avoid.

One of the easiest ways to detect cameras is to use a camera finder.

Camera finders would be more correctly called reflection or lens finders because they use light reflected off camera lenses to find hidden cameras.

These devices typically have a lens or filter that the operator looks through to sweep an area for cameras while the device projects light, which is reflected back by camera lenses and highlighted when the operator looks through the camera finder’s lens or filter which matches the color of light.

Some devices employ magnified lenses and can aid in the detection of cameras at 6′-30′ distance. Some operate in the NIR range so you don’t have to darken the room in order for the device to be effective.

Alternatively, you could use a wireless camera finder, but they only find wireless cameras that are transmitting. You could use a glint finder, but they are really designed to find a camera with a flash by illuminating the retro-reflective material in the flash element, but they can sometimes aid in

finding a lens.

Or you could try a glint finder app. They attempt to employ your smartphone LED as a glint finder, but I yet to see one that I would describe as effective.

Pro’s

- Compact.
- Helps you find cameras to up your situational awareness, improve your security and better avoid them.
- Works on cameras whether they are on or not.
- A simple version of this tools can be improvised out of materials you probably have laying around the house or could buy at a Walmart if you enjoy the thought of hastening the US economy along its charted course. Not one of your many skills? Pull up an Instructable or “How To” article on-line.

Con’s

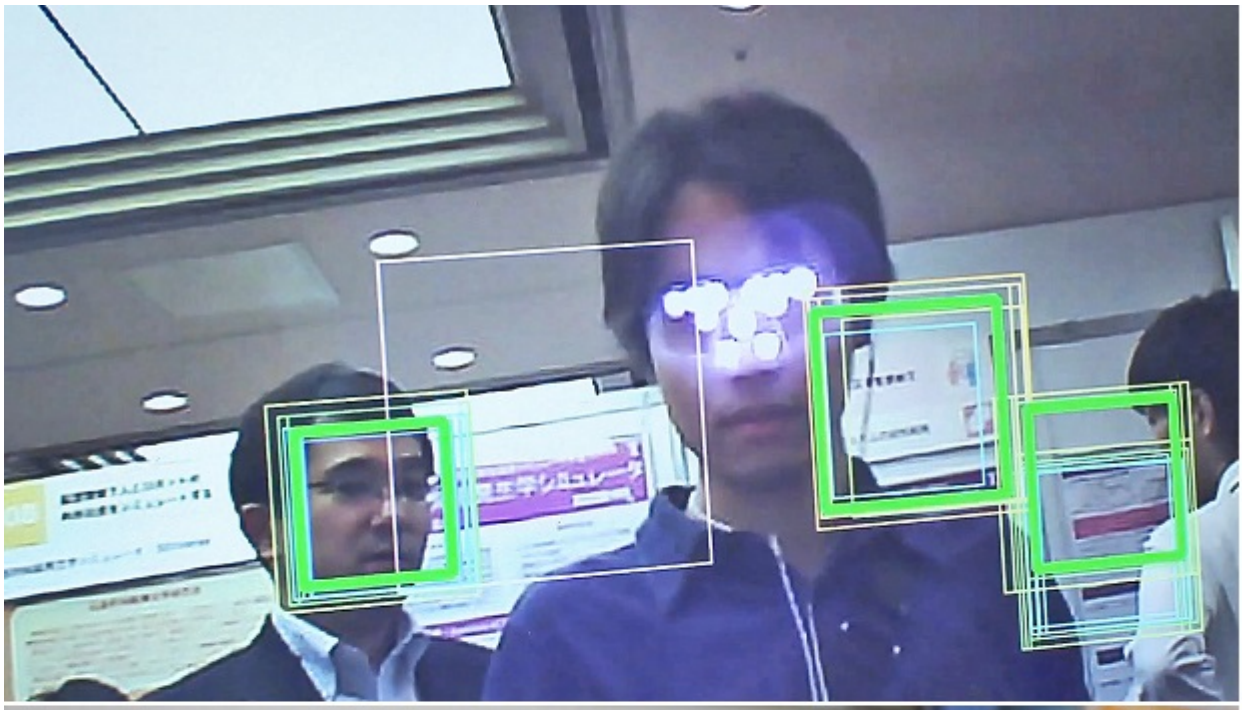
- Won’t find a camera if it is hidden behind a reflective surface like a one-way mirror, so you should inspect any reflective surfaces to make sure they are one-way and don’t have any pinholes.
- Only identifies cameras as opposed to “tricking” facial recognition software.
- The process of sweeping for cameras will seem strange under most circumstances if done in public.
- Today, cameras have lenses, but innovators are working hard on lens-less camera designs that would not be able to be detected by this technology.
- Quality varies.

2. Clothing and Accessories with

NIR LEDs

These products use bright NIR LEDs to overload the light sensors on a digital cameras resulting in unusable images.

According to Kit Eaton at FastCompany, if you wear clothing or accessories that protect your privacy, you are “cartoonishly paranoid.” But manufacturers do not seem to be bothered by liberal media naysayers and are making clothing and accessories with features like NIR LEDs to defeat surveillance and facial recognition cameras.



The first product I saw was a pair of eyeglasses designed by professors Isao Echizen and Seiichi Gohshi of Kogakuin University. They sported an array of 11 NIR LEDs in front of the face to blind digital cameras. Now there are baseball caps, hoods and even a burqa.

Pro’s

- Some are not overtly visible to the naked eye.
- Can be integrated into clothing and accessories.

- Can be a DIY project.

Con’s

- Very obvious on camera that you are using the technology.
- It hides your face as opposed to “tricking” the camera that you are someone else.
- Writers might call you names.

3. Retro-reflective Clothing and Accessories

Wearing clothing that has even a couple of inches of surface area that is retro-reflective makes it trivially easy for anyone with a flashlight or night vision with an IR illuminator to find you in the dark, but it can also blind cameras in much the same way that NIR LEDs do.


Just make sure the material is near your face. Retro-reflective eyeglass frames and hoodies with retro-reflective trim are two effective options.

Certain materials like BlackMagic by 3M do not reflect visible light, but do reflect NIR light.

Pro’s

- Not necessarily overtly visible to the naked eye.
- Good for night signaling in an emergency.
- Good for roadside safety.

Con’s

- Users stand out to searchlights at night.
- Very obvious on camera that you are using the technology.
- It hides your face as opposed to “tricking” the camera that you are someone else.

4. URME Prosthetic Mask

This high quality prosthetic mask of the face of privacy activist Leo Selvaggio is not your typical Halloween mask.

The name is pronounced “U-R-Me” and I believe the mask started

on Indiegogo and may still be available on ThatsMyFace.com. The mask fools Facebook's facial recognition software and are sold at cost because Selvaggio believes that everyone has the right to privacy.

This mask is so high quality that the chances of someone calling you on it on the street are pretty slim as long as nothing looks out of place with the rest of your appearance and you don't have to speak to them. But a facial recognition camera is not going to notice that your lips are not moving.

Pro's

- Convenient.
- Quick change.
- High quality.

Con's

- Expensive at $400.
- "Why are you wearing a mask?"
- If someone stops you, and you speak, they will probably notice that your lips aren't moving.
- Some software may eventually filter out this "face" unless masks of many more faces are made.

5. Hair & Makeup

By styling hair and wearing makeup in certain patterns, facial recognition can be fooled.

Adam Harvey devoted his master's thesis to fooling facial recognition and arrived at the makeup patterns in the image. He says that they work by throwing off the symmetry that the software recognizes as a human face.

If you are going to apply camouflage makeup, why not incorporate a pattern that will fool facial recognition cameras?

Pro's

- Inexpensive.
- Probably not going to motivate someone to call the police and report you.
- DIY.

Con's

- May not work 100% of the time.
- "Why are you dressed like that?"

- Not quick or convenient to change your appearance.

6. Balaclava, Sunglasses & Hat

I always have one or more hats, some quality sunglasses and a balaclava in my EDC bag and use this method to protect my identity in photos I post to social media or when editors, radio shows or Expo's want a head shot.

One of my favorites is a no-drip, fire and flash-resistant flesh tone balaclava of DryMax material, but I have others I wear in cold weather or for specific purposes. I like the Shemaughlava by 782 Gear too and always have a large 100% cotton handkerchief or shemagh handy.

The same tools can help protect you from exposure, protect your eyes or can help protect your identity if you have to do something you're not proud of in a world full of cameras.

When things go sideways and the lights go out, I find comfort in reaching for low tech tools to solve the problems at hand and hats and balaclavas are just that.

If you use this method, be sure to cover as much of your face

as possible. Object recognition does not use the covered portions of your face and some software can identify faces with as little as 30%-50% of the face unobstructed.

Pro's

- Easy to explain why you carry it.
- Low tech.
- Multi-use.
- Inexpensive.
- Practical.

Con's

- Hides you as opposed to "tricking" the camera.
- Will not work with thermal imaging unless you use materials designed to do so such as multi-spectral camouflage.

Whether facial recognition is of the high-tech or low-tech variety, some survivors will be identified with the aid of camera technology, hunted down, tried and punished for crimes…not necessarily in that order, and even if the "crime" was simply being of the wrong political affiliation, race, ethnicity or nationality. This happened in and after the Balkans wars in the 1990's. So prepare and beware!