Soon There Will Be No Place To Hide - The Facial Recognition Revolution

January 16, 2019 - In what can only be called a fools-errand, a large number of consumer advocacy groups including the ACLU and the EFF have now banded together to ask Microsoft, Google and Amazon not to sell their facial recognition software to the federal government. Their concerns run the gamut from personal privacy to targeting illegal aliens, while they ignore the elephant in the room; the lack of any federal legal framework to regulate the use of this technology in both the private and government sectors. Their requests also seem to be oblivious to the fact that Microsoft, Google and Amazon are far from the only players in facial recognition development, and they may not even be the most advanced. Many of the companies that are playing in this market are specifically targeting the federal government because they know it has the potential to become their largest client.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

There is no doubt that facial recognition is changing the world as we know it. The number of places that you can go in private these days is rapidly diminishing. When you drive, there is already a network of cameras across the country that can track your movements in most metropolitan areas. And when you walk into airports, train stations or even your local mall, you're being surveiled on camera.

As with any technology, facial recognition can be used for good and for bad. If it is used to catch criminals, most people would say that's a good thing. But in China, the Chinese government is already using it in conjunction with other tools to crush dissent. Most of us would agree that this is a reprehensible thing. It is pretty clear that it's not the technology that is the issue. It's the way it's used.

At present, the technology - meaning the software - isn't really good enough to use on its own. Some of the most sophisticated platforms have around a 60% accuracy rate. At best, it is good enough to provide the person using it a nudge. Something like, "Hey, I think this is so-and-so." It's up to the operator to do a little digging to confirm or reject the information provided by the software.

But the software is improving rapidly. In ten years, it could have close to 100% accuracy. And since facial recognition is really all about the software and can be run using pretty much any computer and any set of cameras, deploying more accurate software versions will be as simple as an upgrade. The computer and camera networks that exist today will probably work just fine. That makes upgrading a lot less expensive and almost assures that it will happen; protest or not and whether or not Microsoft, Google and Amazon participate in it.

Frankly, I'm more concerned with how the technology will be used in the private sector than I am in government uses. Knowing who is entering or leaving the United States is actually a good thing from my perspective. So is finding wanted criminals. Go figure.

But the private sector is another story entirely. Once facial recognition gets to be a little more accurate, it is only a matter of time before it is used for marketing purposes. It will be able to target you based on what you've been seen shopping for. There are even scenarios that would allow merchants in brick and mortar establishments to offer goods at different prices to different people, based on their known off-line shopping habits.

It will also become valuable information for online shopping. If you are seen shopping in a store for a vacuum today, facial recognition will make it possible to target you online for that same item. Larger retailers will establish databases of facial recognition data that they can use and sell. Smaller retailers will probably rely on outside third party providers for similar services. And criminals are likely to target the databases of both.

The commercial uses for this data pose a much greater risk to the average American than the government uses do. And currently there are few, if any, laws to prevent it.

But going back to today's call by these groups, its worth noting that the Defense Advanced Research Agency (DARPA) is funding multiple companies to develop various facial recognition systems. That technology will belong to the government and the first of those systems is already deployed. A company by the name of Neurala has integrated its software with police body cameras. According to a report in BiometricUpdate the company , "has created patent-pending image recognition and machine learning technology similar to other machine learning methods but far more scalable, so a device carried by a police offer on their shoulder can learn to recognize shapes and â€” potentially faces â€” as quickly and reliably as a much larger and more powerful computer." Other companies and federal agencies are also spending money and working on this technology.

Asking some of the largest technology companies in the country to forgo working with the US government is simply an attempt to shut the barn door. But the horse has already gotten away. The real question is what are lawmakers going to do about it. That's a question that only Congress can answer. And that's probably where these groups should have sent their letter.

byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS