OPENING STATEMENT OF CHAIRMAN FRANKEN “WHAT FACIAL RECOGNITION TECHNOLOGY MEANS FOR PRIVACY AND CIVIL LIBERTIES.”

This hearing will be called to order. Welcome to the fourth hearing of the Subcommittee on Privacy, Technology and the Law. Today’s hearing will examine the use of facial recognition technology by the government and the private sector — and what that means for our privacy and civil liberties.

I want to be clear: there is nothing inherently right or wrong with facial recognition technology. Just like any other new and powerful technology, it is a tool that can be used for great good. But if we do not stop and carefully consider the way we use this technology, it may also be abused in ways that could threaten basic aspects of our privacy and civil liberties. I called this hearing so we can start that conversation.

I believe that we have a fundamental right to control our private information--and biometric information is already among the most sensitive of our private information, mainly because it is both unique and permanent. You can change your password. You can get a new credit card. But you can’t change your fingerprint, and you can’t change your face. Unless I guess you go to a great deal of trouble.

Indeed, the dimensions of our faces are unique to each of us—just like our fingerprints. And just like fingerprint analysis, facial recognition technology allows others to identify you with what’s called a “faceprint,” a unique file describing your face.

But facial recognition creates acute privacy concerns that fingerprints do not. Once someone has your fingerprint, they can dust your house or your surroundings to figure out what you’ve touched.

Once someone has your faceprint, they can get your name, they can find your social networking account and they can find and track you in the street, in the stores you visit, the government buildings you enter, and the photos your friends post online. Your face is a conduit to an incredible amount of information about you. And facial recognition technology can allow others to access all of that information from a distance, without your knowledge and in about as much time as it takes to snap a photo.

People think of facial recognition as something out of a science fiction movie. In reality, facial recognition technology is in broad use today. If you have a drivers’ license, if you have a passport, if you are a member of a social network, chances are good that you are part of a facial recognition database.

There are countless uses of this technology, and many of them are innovative and quite useful. The State Department uses facial recognition technology to identify and stop passport fraud—preventing people from getting multiple passports under different names. Using facial recognition technology, Sheriff Larry Amerson of Alabama, who is with us here today, can make sure that a prisoner being released from the Calhoun County jail is actually the same prisoner that is supposed to be released. Similarly, some of the latest smartphones can be unlocked by the owner by just looking at the phone and blinking.

But there are uses of this technology that should give us pause.

In 2010, Facebook, the world's largest social network, began signing up all of its then-800 million users in a program called Tag Suggestions. Tag Suggestions made it easier to tag close friends in photos. That's a good thing.

But the feature did this by creating a unique faceprint for every one of those friends. And in doing so, Facebook may have created the world's largest privately-held database of faceprints--without the explicit consent of its users. To date, Tag Suggestions is an opt-out program. Unless you have taken the time to turn it off, it may have already been used to generate your faceprint.

Separately, last year, the FBI rolled out a facial recognition pilot program in Maryland, Michigan and Hawaii that will soon expand to three more states. This pilot lets officers in the field take a photo of someone and compare it to a federal database of criminal mugshots. The pilot can also help ID a suspect in a photo from an actual crime. Already, several other states are setting up their own facial recognition systems independently of the FBI. These efforts will catch criminals: they already have.

Now many of you may be thinking that that's an excellent thing. I agree. But unless law enforcement facial recognition programs are deployed in a very careful manner, I fear that these gains could eventually come at a high cost to our civil liberties.

I fear that the FBI pilot could be abused to not only identify protesters at political events and rallies, but to target them for selective jailing and prosecution, stifling their First Amendment rights. Curiously enough, a lot of the presentations on this technology by the Department of Justice show it being used on people attending political events or other public gatherings.

I also fear that without further protections, facial recognition technology could be used on unsuspecting civilians innocent of any crime — invading their privacy and exposing them to potential false identifications.

Since 2010, the National Institute of Justice, which is a part of DOJ, has spent $1.4 million to develop facial recognition-enhanced binoculars that can be used to identify people at a distance and in crowds. It seems easy to envision facial recognition technology being used on innocent civilians when all an officer has to do is look at them through his binoculars.

But facial recognition technology has reached a point where it is not limited to law enforcement and multi-billion dollar companies: it can also be used by private citizens. Last year, Professor Alessandro Acquisti of Carnegie Mellon University, who is testifying today, used a consumer-grade digital camera and off-the-shelf facial recognition software to identify one out of three students walking across a campus.

I called this hearing to raise awareness about the fact that facial recognition already exists right here, today, and we need to think about what that means for our society. I also called this hearing to call attention to the fact that our federal privacy laws are almost totally unprepared to deal with this technology.

Unlike what we have in place for wiretaps and other surveillance devices, there is no law regulating law enforcement use of facial recognition technology. And current Fourth Amendment case law generally says that we have no reasonable expectation of privacy in what we voluntarily expose to the public — yet we can hardly leave our houses in the morning without exposing our faces to the public. So law enforcement doesn't need a warrant to use this technology on someone. It might not even need to have a reasonable suspicion that the subject has been involved in a crime.

The situation for the private sector is similar. Federal law provides some protection against true bad actors that promise one thing yet do another. But that's pretty much as far as the law goes. If a store wants to take a photo of your face when you walk in and generate a faceprint — without your permission — they can do that. They might even be able to sell it to third parties.

Thankfully, we have a little time to do better. While this technology will in a matter of time be at a place where it can be used quickly and reliably to identify a stranger, it isn't there just yet. And so I have called the FBI and Facebook here today to challenge them to use their position as leaders in their fields to set an example for others—before this technology is used pervasively.

The FBI already has some privacy safeguards in place. But I still think that they could do more to prevent this technology from being used to identify and target people engaging in political protests or other free speech. I think the FBI could do more to make sure that officers use this technology only when they have good reason to think that someone is involved in a crime. I also think that if the FBI did these things, law enforcement agencies around the country would follow.

For their part, Facebook allows people to use Tag Suggestions only on their close friends. But I think Facebook could still do more to explain to its users how it uses facial recognition — and to give them better choices about whether or not to participate in Tag Suggestions. I think that Facebook could make clear to its users just how much data it has—and how it will and will not use its large and growing database of faceprints. And I think that if Facebook did these things, they would establish a best practice against which other social networks would be measured.

My understanding is that for the past few months, Facebook Tag Suggestions has been temporarily disabled to allow for some technical maintenance. It seems to me that Facebook has the perfect opportunity to make changes to its facial recognition program when it brings Tag Suggestions back online.

I'm also calling the Federal Trade Commission to testify because they are in the process of actually writing best practices for the use of this technology in industry. I urge the Commission to use this as an opportunity to guarantee consumers the information and choices they need to make informed decisions about their privacy.

In the end, though, I also think that Congress may need to act — and it wouldn't be the first time it did. In the era of J. Edgar Hoover, wiretaps were used freely with little regard to privacy. Under some Supreme Court precedents of that era, as long as the wiretapping device did not actually penetrate the person's home or property, it was deemed constitutionally sound — even without a warrant. And so in 1968, Congress passed the Wiretap Act. Thanks to that law, wiretaps are still used to stop violent and serious crimes. But police need a warrant before they get a wiretap. And you can't wiretap someone just because they're a few days late on their taxes — wiretaps can be used only for certain categories of serious crimes.

I think that we need to ask ourselves whether Congress is in a similar position today as it was 50 or 60 years ago—before passage of the Wiretap Act. I hope the witnesses today will help us consider this and all of the different questions raised by this technology. With that, I will turn to my friend and the Ranking Member, Senator COBURN.