technology. That didn't happen with wiretaps, or geolocation, or any other surveillance technology.

That changed with face recognition. For the first time, cities and states put near total bans or moratoria on government use of a surveillance technology. I think it's worth sitting with that for a second: biometric surveillance technology is so sensitive that American legislatures tried to rein it in in a way that they never had before.

Of course, those measures focused on government use of the technology—not corporate use of biometrics, which raises a related but also separate set of issues. Which is one reason I'm so excited about today's statement:

With today's statement, we are setting clear guideposts for how our oldest consumer protection authority—Section 5 of the FTC Act—applies to commercial use of biometric technology.

I want to be clear: This is our view on how one law applies to biometrics. We enforce around 80 laws. And so it is entirely possible that other rules would apply based on those other statutes.

Biometrics is an area mired in technical jargon: "Probe images," "false posie("f)-1 2m on thatu"fals

Third, it is *common knowledge* that this technology can be biased. Companies cannot ignore that. They need to take proactive steps to reduce or eliminate the risks that such errors could hurt people.

And so if you are a company using biometric technology, you need to think about how biases in that technology will affect the public. And you need to address any substantial consumer harm that may flow from that.

Lastly, and most importantly, there are some uses of this technology that are illegal in and of themselves.

If you are tracking highly sensitive information that could be used to hurt people, if you are doing it in secret such that people cannot avoid that, I urge you to consider whether you should be using that technology in the first place.