The New York Times https://nyti.ms/2G76rNq

We're Banning Facial Recognition. We're Missing the Point.

The whole point of modern surveillance is to treat people differently, and facial recognition technologies are only a small part of that.

By Bruce Schneier
Mr. Schneier is a fellow at the Harvard Kennedy School.

Jan. 20, 2020

Communities across the United States are starting to ban facial recognition technologies. In May of last year, San Francisco banned facial recognition; the neighboring city of Oakland soon followed, as did Somerville and Brookline in Massachusetts (a statewide ban may follow). In December, San Diego suspended a facial recognition program in advance of a new statewide law, which declared it illegal, coming into effect. Forty major music festivals pledged not to use the technology, and activists are calling for a nationwide ban. Many Democratic presidential candidates support at least a partial ban on the technology.

These efforts are well intentioned, but facial recognition bans are the wrong way to fight against modern surveillance. Focusing on one particular identification method misconstrues the nature of the surveillance society we're in the process of building. Ubiquitous mass surveillance is increasingly the norm. In countries like China, a surveillance infrastructure is being built by the government for social control. In countries like the United States, it's being built by corporations in order to influence our buying behavior, and is incidentally used by the government.

In all cases, modern mass surveillance has three broad components: identification, correlation and discrimination. Let's take them in turn.

Facial recognition is a technology that can be used to identify people without their knowledge or consent. It relies on the prevalence of cameras, which are becoming both more powerful and smaller, and machine learning technologies that can match the output of these cameras with images from a database of existing photos.

But that's just one identification technology among many. People can be identified at a distance by their heart beat or by their gait, using a laser-based system. Cameras are so good that they can read fingerprints and iris patterns from meters away. And even without any of these technologies, we can always be identified because our smartphones broadcast unique numbers called MAC addresses. Other things identify us as well: our phone numbers, our credit card numbers, the license plates on our cars. China, for example, uses multiple identification technologies to support its surveillance state.

Once we are identified, the data about who we are and what we are doing can be correlated with other data collected at other times. This might be movement data, which can be used to "follow" us as we move throughout our day. It can be purchasing data, internet browsing data, or data about who we talk to via email or text. It might be data about our income, ethnicity, lifestyle, profession and interests. There is an entire industry of data brokers who make a living analyzing and augmenting data about who we are — using surveillance data collected by all sorts of companies and then sold without our knowledge or consent.

There is a huge — and almost entirely unregulated — data broker industry in the United States that trades on our information. This is how large internet companies like Google and Facebook make their money. It's not just that they know who we are, it's that they correlate what they know about us to create profiles about who we are and what our interests are. This is why many companies buy license plate data from states. It's also why companies like Google are buying health records, and part of the reason Google bought the company Fitbit, along with all of its data.

The whole purpose of this process is for companies — and governments — to treat individuals differently. We are shown different ads on the internet and receive different offers for credit cards. Smart billboards display different advertisements based on who we are. In the future, we might be treated differently when we walk into a store, just as we currently are when we visit websites.

The point is that it doesn't matter which technology is used to identify people. That there currently is no comprehensive database of heart beats or gaits doesn't make the technologies that gather them any less effective. And most of the time, it doesn't matter if identification isn't tied to a real name. What's important is that we can be consistently identified over time. We might be completely anonymous in a system that uses unique cookies to track us as we browse the internet, but the same process of correlation and discrimination still occurs. It's the same with faces; we can be tracked as we move around a store or shopping mall, even if that tracking isn't tied to a specific name. And that anonymity is fragile: If we ever order something online with a credit card, or purchase something with a credit card in a store, then suddenly our real names are attached to what was anonymous tracking information.

Regulating this system means addressing all three steps of the process. A ban on facial recognition won't make any difference if, in response, surveillance systems switch to identifying people by smartphone MAC addresses. The problem is that we are being identified without our knowledge or consent, and society needs rules about when that is permissible.

Similarly, we need rules about how our data can be combined with other data, and then bought and sold without our knowledge or consent. The data broker industry is almost entirely unregulated; there's only one law — passed in Vermont in 2018 — that requires data brokers to register and explain in broad terms what kind of data they collect. The large internet surveillance companies like Facebook and Google collect dossiers on us more detailed than those of any police state of the previous century. Reasonable laws would prevent the worst of their abuses.

Finally, we need better rules about when and how it is permissible for companies to discriminate. Discrimination based on protected characteristics like race and gender is already illegal, but those rules are ineffectual against the current technologies of surveillance and control. When people can be identified and their data correlated at a speed and scale previously unseen, we need new rules.

Today, facial recognition technologies are receiving the brunt of the tech backlash, but focusing on them misses the point. We need to have a serious conversation about all the technologies of identification, correlation and discrimination, and decide how much we as a society want to be spied on by governments and corporations — and what sorts of influence we want them to have over our lives.

Bruce Schneier is a fellow at the Harvard Kennedy School and the author, most recently, of "Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World."