Speaking at a conference two years ago, Microsoft’s CEO displayed a slide featuring the book jackets of 1984 and Brave New World. “I do believe it’s up to us to ensure that some of the more dystopian scenarios don’t come true,” Satya Nadella said. Too late. The surveillance dystopia is on the horizon, and companies like Microsoft and Amazon are helping build it. Despite their platitudes of caution and ethics, we’ve seen the consequences of Silicon Valley’s “move fast and break things” ethos. And if we don’t stop the spread of facial recognition, its latest lucrative surveillance product, we’ll soon count our most basic freedoms among the things they’ve broken. Academics have called facial recognition, the use of artificial intelligence to pick out and identify individuals from vast databases, “the most uniquely dangerous surveillance mechanism ever invented.” And with quickly spreading commercial products like FaceApp and Facebook’s Face-ID raising privacy alarm bells, it’s easy to see how quickly we’ll feed this beast once it’s unleashed. That’s why my organization Fight for the Future is launching a nationwide campaign to shine a spotlight on where facial recognition surveillance is already happening, and how people can act at the local, state, and federal levels to stop it. Company after company in Silicon Valley has been pushing furiously ahead with the development of face-scanning surveillance tools. They see money to be made selling this tech to governments, airlines, and other private businesses. Facing growing concern from the public and lawmakers, the industry has disingenuously asked for “regulation.” This is straight out of Big Tech’s lobbying playbook — asking Congress to pass laws and then swooping in to help write them. By doing so, they hope to avoid the real debate: whether facial recognition surveillance should be allowed at all. The answer is clearly no. The threat that facial recognition poses to human society and basic liberty far outweighs any potential benefits. It’s on a very short list of technologies — like nuclear and biological weapons — that are simply too dangerous to exist, and that we would have chosen not to develop had we had the foresight. Silicon Valley, however, continues to forge ahead, bidding on lucrative government contracts that are already enabling surveillance, the likes of which we’ve never seen. We are on the verge of an unprecedented increase in state and private spying that will be built in plain sight. It will be built in winsome partnership between corporations and government agencies hungry for more data and control. The rich will grow richer, unaccountable authorities will become more powerful, and the rest of us will be subject to deeply invasive monitoring every time we leave our homes. Tech lobbyists acknowledge some of the flaws in current facial recognition products, but promise they can be fixed or addressed with industry-friendly regulation. But even if these algorithms worked perfectly, ubiquitous face scanning still poses an enormous threat to the future of human freedom. Biometric surveillance powered by artificial intelligence is categorically different than any surveillance we have seen before. It enables real-time location tracking and behavior policing of an entire population at a previously impossible scale. Consider Slate’s reporting on the algorithms that review security camera footage. They look for “triggers,” which could include “complex and nuanced emotional and cognitive states” registered by your expressions. As ominous as it is to imagine a person you’ve never met watching your every move — comparing you to mugshots and anticipating whether you’ll commit a crime — imagine instead software working at top speed and incapable of empathizing with you. It thinks it knows how you feel and what you intend. It doesn’t care if you’ve had a bad day. That look on your face could peg you as an enemy of the state. Any one of us could become the victim of an algorithm’s cold testimony. There is no amount of regulation, transparency, or oversight that will fix the dangers inherent in widespread face surveillance. Only a full ban — a federal ban, covering the use of facial recognition by government agencies, in public places, and in public contracts with private entities — can prevent our nightmares from becoming reality. As terrifying as a vision of accurate surveillance technology is, the technology’s current shortcomings are scary enough. Facial recognition algorithms systematically misidentify people of color and women as criminals, automating existing forms of discrimination and profiling. The sheer pace and scale at which such targeting can soon occur will lead to increased police harassment and false arrests, filling our prisons even faster, with centuries of racism built into the software. Just last weekend, we learned that immigration authorities were scouring state databases of driver’s licenses, scanning millions of Americans’ faces without any consent in an attempt to locate and deport undocumented immigrants. In some cases, they targeted undocumented people who had legally obtained drivers licenses in states where they are allowed to do so, a devastating bait and switch. The good news is that, while facial recognition is spreading at an alarming pace, momentum against it is growing. San Francisco, Oakland, and Somerville, Massachusetts, recently became the first cities in the country to ban the technology. Berkeley is also considering a ban, and bills to halt current use of the tech are before the Massachusetts and Michigan legislatures. In Congress, there is growing bipartisan agreement to address the issue, but it could easily stall under pressure from law enforcement and Big Tech. There is no time to waste. Authoritarian surveillance programs are always used to target the most vulnerable and marginalized, and facial recognition enables the automation of oppression.