POLICY & LAW

HOW SHOULD WE REGULATE FACIAL RECOGNITION?

We asked the experts

By Russell Brandom @russellbrandom Aug 29, 2018, 10:13am EDT

Illustrations by Alex Castro

Facial recognition is everywhere — airports, police stations, and built into the largest cloud platforms in the world — with few federal rules to govern how it's used. That's been true for years, but a string of embarrassing stories in recent months has driven home exactly how dangerous the technology can be in the wrong hands, and it's led to new calls for regulation. Even Microsoft, one of the largest providers, has called on Congress to place some kind of restriction on how and where the technology can be used.

A truly effective facial recognition law would have to tackle several problems at once. Many facial recognition algorithms still show higher error rates for African-Americans, women, and young people, suggesting the systems might be entrenching societal biases. Beyond bias, the sheer power of facial recognition as a surveillance tool has led some groups to call for a moratorium on police use. And now that the technology is accessible to anyone with a cloud developer account, the private sector privacy issues are even harder to ignore.

That leaves reformers with a difficult question: how can we fix facial recognition? We put the question to five leading figures on both sides of the policy fight.

IS IT TIME TO REGULATE FACIAL RECOGNITION?

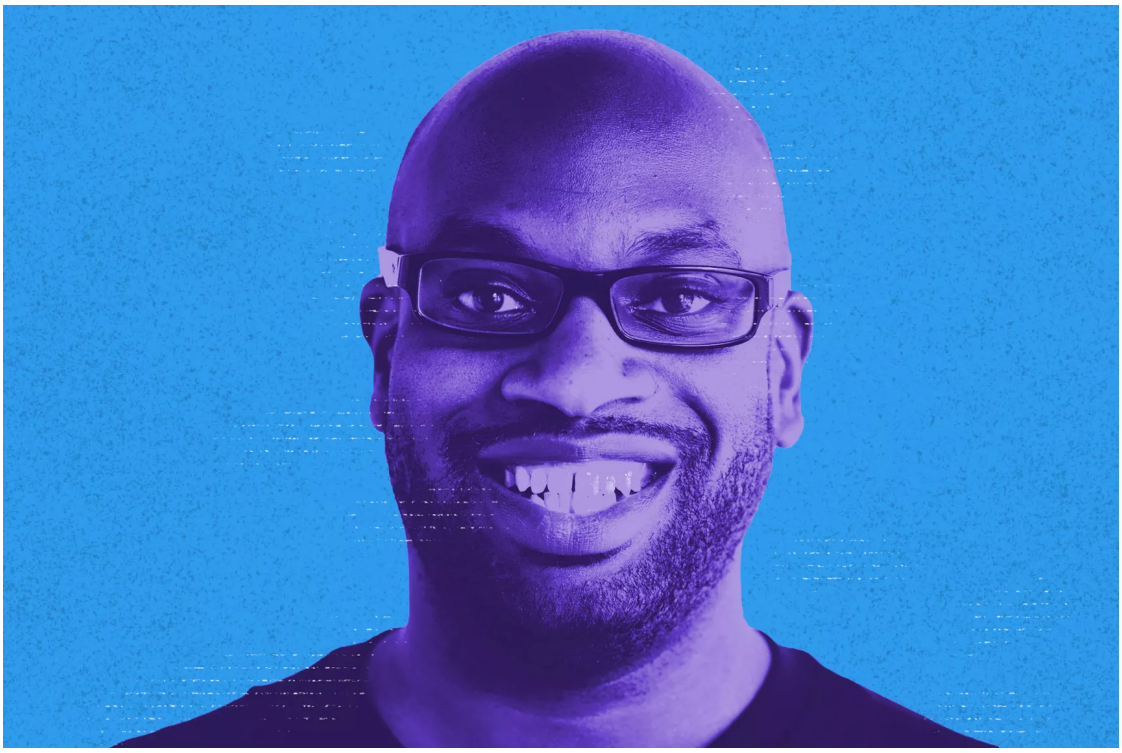
Alvaro Bedoya, executive director of the Center for Privacy and Technology at Georgetown Law. The Center's Perpetual Lineup project includes a model bill for regulating facial recognition, focused on restricting police access to driver's license and mug shot databases.

We regulate commercial privacy on any number of other technologies. Credit cards, we regulate them. E-health records, we regulate them. Your cable viewing habits, protected. Your video rental habits, protected. So this idea that just because it's a technology, we shouldn't regulate it doesn't fit with the entirety of the US commercial privacy landscape. It's never been an argument in commercial privacy to say to Congress, "Oh, this is a technology. It's just ones and zeroes. You shouldn't really regulate it." And it's already regulated for 1 out of 8 Americans. In Illinois and Texas, the rule is to get permission. So there's precedent for it both in how we regulated commercial privacy in the past and how we already regulate face recognition today. And I think the simple rule of getting people's permission makes a ton of sense.

Beyond that, I'd like to see rules around bias and accuracy testing. You probably want protections for children. It should probably not be used on people who are 18 or younger. You probably want prohibitions on sensitive areas like hospitals or clinics or schools, where even if someone's consented, you still shouldn't use it.

Look at surveillance cameras. You do not usually have surveillance cameras in bathrooms. You can have them all throughout the store, you'll have them at the entrance, the exit, in the aisles, at the checkout. But you do not have them in the bathroom because we all understand that recording people in the bathroom is a bad idea.

Brian Brackeen, CEO of the facial recognition company Kairos, an outspoken advocate for regulation in the industry.



I can't wait for regulation. We're big proponents of regulation, going back to the NTIA working group. There is a need for regulation in this space, both for law enforcement and even private companies in certain use cases. We're not opposed to consent requirements either. Particularly in private sector use, there is a relationship between our customer and the individual, so they should be able to get consent. In our case, we have a lot of banking clients. We're verifying a transaction using the customer's face. There's obviously a relationship there, and there's a value to the customer in not being the subject of fraud. So for our use case, there's no problem getting consent. But when you're Facebook or you're Amazon and you're using this for the government or trying to bait-and-switch from photos you already have, that's a different thing. And that's why they were so against it.

What we need is the NTIA process with an anvil over our head. We need to say, "We're doing regulation in the fourth quarter. This is the first quarter, so you have a year to give us best practices." So let's get people in a room working through these issues with that requirement over our heads. I do think there is a will for it from both sides, Republicans and Democrats.

Evan Selinger, philosophy professor at the Rochester Institute of Technology. Together with law professor Woodrow Herzog, Selinger has called for a complete ban on the use of facial recognition, in both public and private use cases, out of concern that the technology is being normalized.

The important question to ask is: what does it take to get the public on board with a massive facial recognition infrastructure? The answer is normalization. Get people used to using the technology all the time. Don't just make them comfortable with facial recognition technology, engineer the desire for it. Create habits that lead people to believe they can't live without facial recognition tech in their lives. This is what the consumer side of facial recognition technology is doing: making it seem banal and unworthy of concern. By getting people to see facial recognition technology as nothing extraordinary, an argument about value and risk is being made.

Benji Hutchinson, VP of federal operations at NEC America. A leading vendor for federal facial recognition contracts, NEC has resisted calls for federal restrictions on the technology.

We do not believe in a complete moratorium on the technology, and we do not believe that there is a burning need for over-legislation. A lot of the positions that we're seeing are coming from tech companies that are new to the space. And I would argue that these large companies are a little bit on their heels. They're trying to do all they can do to make sure that they don't lose the contracts they have and do the right thing. I don't fault them altogether, but I don't necessarily agree with the approach.

People forget the benefits. That gets drowned out. This is a wildly successful technology that's been used to stop terror attacks. It's been used to take criminals off the street. It lets us have paperless, frictionless travel when we're going through airports. It decreases lines and wait times. It makes people's lives better. And I think those benefits get lost in all the negativity.

SHOULD POLICE USE FACIAL RECOGNITION?

Kade Crockford, director of the Technology for Liberty Program at the ACLU of Massachusetts. The ACLU has called for a moratorium on government use of facial recognition.

Our core concern is that policing in the United States today functions without effective oversight or accountability. There's a real deficit of trust. And in that ecosystem, it's really hard to see how any legal requirement could be applied in a way that would truly protect people.

If police want to conduct a wiretap, they have to go to a judge and get a wiretap order, which is like a super-warrant. And they take that wiretap order to a phone company. Under federal law, the phone company is not allowed to disclose information absent from that wiretap order. So there's a kind of built-in protection there. The phone company could be liable if they allow police to wiretap you without an order, and the actual infrastructure that facilitates the surveillance is not in the possession of law enforcement. It belongs to this third party, the phone company. So there's a built-in check there.

We do not have a parallel track for face surveillance. What law enforcement wants, and what it seems like Amazon is trying to push on police departments nationwide, is the creation of this infrastructure inside the police department. We just don't have the civil society or governmental infrastructure to ensure that law enforcement would not abuse that.

Brackeen: Police have both the question and the answer. When I'm doing banking and commercial applications, my customers don't have databases of everybody's photo, so they can't just put a camera in the front of a store and know everybody who's walking by. But if I am the City of Orlando and I have everyone's driver's license plus access to the FBI's database, then I can put a camera on Main Street and know everybody who's walking by. So the government has an ability that's beyond other folks.

Then there's the bias issue. If you have a tool like a stun gun and I told you that stun gun only works on women, then you wouldn't allow police to use it, for obvious reasons. The tools of policing need to be equitable across all people, and that's true of AI in general. I want to get to a place where police can use a tool like this and have it be equitable. But I would still have several limitations to that use.

CAN FACIAL RECOGNITION OVERCOME RACIAL BIAS?

Bedoya: The idea that this technology is being used to catch shoplifters when it's documented to not work as well on young people and it's documented to not work as well on African-Americans is just crazy. Every researcher that looks at this finds that there is bias of some sort. It's crazier in the law enforcement context, but it's still pretty crazy in the private sector context. So that's one critical thing I would like to see.

Brackeen: This is not an intractable problem. It's a data problem, not a problem with the technology. We're updating our algorithms ourselves, and we can remove bias, at least up to a point. I think the current outrage is, we're a small company, but we're doing the work necessary to be better. A company like Amazon has always had the resources to do better. But, in fact, they're not, and they're selling to the government.

Hutchinson: If you talk to any big players in the facial recognition space, all of them will say that we have very rigorous testing methodologies. And that includes ethnic individuals in a heterogeneous database. We look for diversity, and we test for it in our algorithms. We spend millions of dollars a year looking for error rates that occur with different types of faces. And those different types of faces can mean a lot of different things. People with different backgrounds, from different regions of the world, different shades, we do all of that testing. We don't publish a lot of the results, but it is absolutely

in our best interest to ensure that it is a low-error algorithm. The fact is, the math is not biased, it's not racist. If some companies have lower-end algorithms and they haven't put the R&D into it and they do have higher error rates with certain ethnic groups, that may just be an issue of a poor algorithm.

Crockford: There's a problem with the algorithms and the training data being biased, but that's not the only problem with bias in this technology. The other problem is that police are using mug shot files as the comparison database, and mug shots are themselves biased because of the degree to which policing has been enacted in a disproportionate manner throughout history and up to the present.

We see disproportionate arrests of black and brown people in almost every category of minor offense, whether it's driving with a suspended license or an expired registration, drug possession, petty larceny, trespassing, disorderly conduct. The bias in marijuana arrests is just astonishing. Even today, 90 percent of the people arrested for marijuana offenses in New York are black or brown. And that's not because white people don't smoke pot in public in New York City. It's just because white people are almost never arrested for that crime. So that is a bias, and by using that database and pretending it's a neutral technology, it codifies that bias. ■

CIRCUIT BREAKER

Nintendo Switch is getting a Fortnite bundle with exclusive items

APPS

Instagram will use ads to help users register to vote

GOOGLE

Google is giving up some control of the AMP format

View all stories in Tech