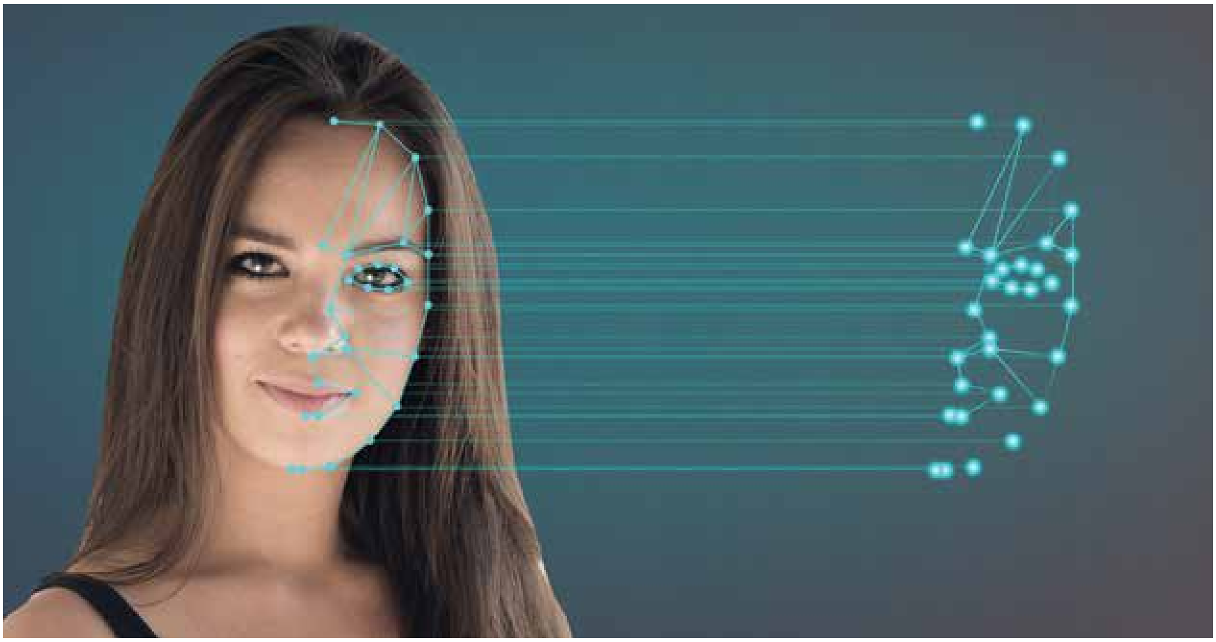
Facial Recognition in 2020:

Can Tech Giants Stop its Regulation?

Civil liberties activists warn that the powerful technology, which identifies people by matching a picture or video of a person's face to databases of photos, can be used to passively spy on people without any reasonable suspicion or their consent. Many of these leaders don't just want to regulate facial recognition tech — they want to ban or pause its use completely.

Republican and Democratic lawmakers, who rarely agree on anything, are in agreement on limiting law enforcement agencies' ability to surveil Americans with this technology, citing concerns that the unchecked use of facial recognition could lead to the creation of an Orwellian surveillance state.

Several cities, such as San Francisco, Oakland, and Somerville, Massachusetts banned police use of the technology last year. A new federal bill was introduced in 2019 that would severely restrict its use by federal law enforcement, requiring a court order to track people for longer than three days. And some senators have discussed a far-reaching bill that would completely halt



government use of the technology.

But the reality is that this technology already exists — it's used to unlock people's iPhones, scan flight passengers faces instead of their tickets, screen people attending musical concerts, and to monitor large crowds.

Its prevalence has created a delicate situation: proponents of the tech, such as law enforcement and technology manufacturers, downplay facial recognition's power. They play up its potential to crack open cold criminal cases or reunite missing children with their families.

Meanwhile, opponents warn of how quickly the powerful tech's use could spiral out of control. For instance, they point to China, where the technology is regularly used to surveil and oppress an ethnic minority. The solution may be somewhere in between — there are cases when use of this tech can do good, especially if it's carefully regulated and the communities impacted by it are in control of how it's used. But right now, that looks like an ideal scenario that we're still far from achieving.

"What we really need to do as a society is sort through what are the beneficial uses of this technology and what are the accompanying harms — and see if there are any roles for its use right now," Barry Friedman, faculty director of NYU Law's Policing Project, a research institute that studies policing practices, told Recode.

Rolling out government use of facial recognition the right way, tech policy leaders and civil liberties advocates say, will involve a sweeping set of regulations that democratize input on how these technologies are used.

The daily use

The most famous examples of law enforcement's use of facial recognition in the US are the extreme ones — such as when police in Maryland used it to identify the suspected shooter at the Capital Gazette newspaper offices.

But the reality is, as many as one in four police departments across the US can access facial recognition according to the Center of Privacy and Technology at Georgetown Law. And at least for now, it's often in more routine criminal investigations.

A report from Gizmodo last January suggested that Washington County police were using the tool differently than how Amazon recommended and had lowered the confidence threshold for a match to below 99 percent.

In the absence of facial recognition regulation, it's easy to see the potential for overreach. In a 2017 interview with tech media company SiliconANGLE, Chris Adzima, a senior information systems analyst for the department, spoke about how video footage can enhance the tool's capabilities — even though the department currently says it has no plans to use video in its surveillance.

Washington County is just one of hundreds of law enforcement agencies at the local, state, and federal level that use facial recognition. And because it uses Rekognition — a product made by Amazon, perhaps the biggest and most scrutinized tech giant — police there have been more public about its use than other law enforcement agencies that use similar, but less known, tools.

Some law enforcement agencies are simply worried that sharing more information about the use of facial recognition will spark backlash, Daniel Castro, vice president of the DC-based tech policy think tank, Information Technology and Innovation Foundation (ITIF), told Recode.

Much of the fear about facial recognition technology is because the public knows little about how it's used, or whether it's been effective in reducing crime. In absence of any kind of systemic federal regulation or permitting process — the little we know is from stories, interviews, public reports, and investigative reports about its prevalence.

And even for police departments that are forthright about how they use the technology, like Washington County, they often don't collect or share any tangible metrics about its effectiveness.

Friedman said that with better data, the public might have a better understanding of the true value of facial recognition technology, and if it's worth the risks.

The bias problem

For racial minorities and women, facial recognition systems have proven disproportionately less accurate. In a 2018 study, MIT Media Lab researcher Joy Buolamwini found that three leading facial recognition tools — from Microsoft, IBM, and Chinese firm Megvii, were incorrect as much as a third of the time in identifying the gender of darker skinned women, as compared to having only a 1 percent error rate for white males.

Amazon's Rekognition tool in particular has been criticized for displaying bias after the ACLU ran a test on the software that misidentified 28 members of Congress as criminals, disproportionately providing false matches for black and Latino lawmakers. Amazon has said that the correct settings weren't used in the ACLU's test because the organization set the acceptable confidence threshold to 80 percent — although it was later reported that this is the default setting in the software, and one that some police departments seem to be using in training materials.

Presumably, bias issues in facial recognition will improve over time, as the technology learns and data sets improve. Meanwhile, proponents argue that while facial recognition technology in its current state isn't completely bias-free, neither are human beings.

And facial recognition can be harder to hold accountable than a human being when it makes a mistake. "If an individual officer is discriminating against a person, there's a through line or a causal effect you can see there, and try to mitigate or address that harm," said Rashida Richardson, director of policy research at AI Now Institute, "But if it's a machine learning system, then who's responsible?"

Much of the fear about facial recognition technology is because the public knows little about how it's used, or whether it's been effective in reducing crime.

The technology that determines a match in facial recognition is essentially a black box — the average person doesn't know how it works, and often the untrained law enforcers using it don't either. So unwinding the biases built into this tech is not a simple task.

Some tech companies, such as Microsoft and IBM, have called for government regulation on the technology. Amazon said earlier this year that it's writing its own set of rules for facial recognition that it hopes federal lawmakers will adopt. But that raises the question: Should people trust companies any more than police to self-regulate this tech?

Other groups such as the ACLU have created a model for local communities to exert oversight and control over police use of surveillance technology, including facial recognition. The Community Control over Police Surveillance laws, which the ACLU developed as a template for local regulation, empowers city councils to decide what surveillance technologies are used in their area, and mandate community input. More than a dozen cities and local jurisdictions have passed such laws, and the ACLU says efforts are underway in several others.

Overall, there may be benefits of law enforcement's use of facial recognition technology — but so far, Americans are relying on police department anecdotes with little data points or accountability. As long as police departments continue to use facial recognition in this information vacuum, the backlash against the technology will likely grow stronger, no matter the potential upside.

Passing robust federal level legislation regulating the tech, working to eradicate the biases around it, and giving the public more insight into how it functions, would be a good first step toward a future in which this tech inspires less fear and controversy.

(Source: This an abridged version of the original article written by Shirin Ghaffary for Recode website.)