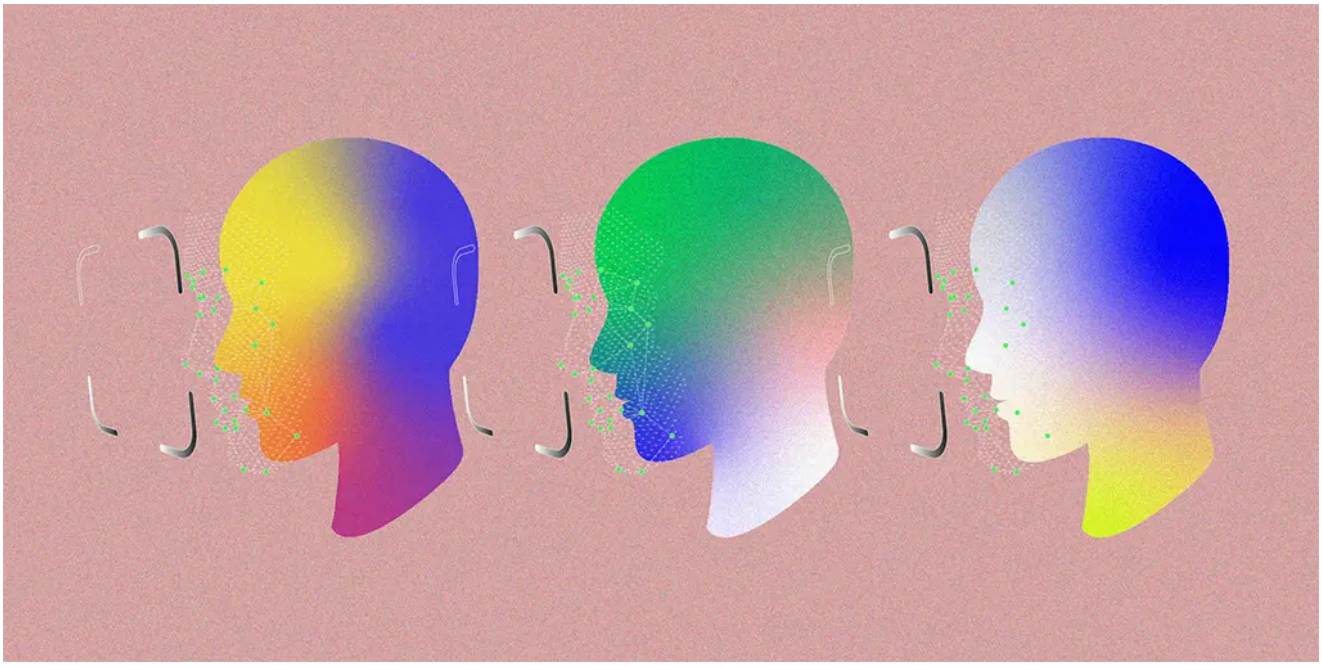
Facial Recognition Is Everywhere. Here's What We Can Do About It.

nytimes.com/wirecutter/blog/how-facial-recognition-works/

Thorin Klosowski



Published July 15, 2020

Facial recognition—the software that maps, analyzes, and then confirms the identity of a face in a photograph or video—is one of the most powerful surveillance tools ever made. While many people interact with facial recognition merely as a way to unlock their phones or sort their photos, how companies and governments use it will have a far greater impact on people's lives.

When it's a device you own or software you use, you may be able to opt out of or turn off facial recognition, but the ubiquity of cameras makes the technology increasingly difficult to avoid in public. Concerns about that ubiquity, amplified by evidence of racial profiling and protester identification, have caused major companies, including Amazon, IBM, and Microsoft, to put a moratorium on selling their software to law enforcement. But as moratoriums expire and the technology behind facial recognition gets better and cheaper, society will need to answer big questions about how facial recognition should be regulated, as well as small questions about which services we're each willing to use and which privacy sacrifices we're each willing to make.

How facial recognition software works

Most people have seen facial recognition used in movies for decades (video), but it's rarely depicted correctly. Every facial recognition system works differently—often built on proprietary algorithms—but you can sort out the process into three basic types of technology:

- *Detection* is the process of finding a face in an image. If you've ever used a camera that detects a face and draws a box around it to auto-focus, you've seen this technology in action. On its own, it isn't nefarious—face detection only focuses on finding a face, not the identity behind it.
- *Analysis (aka attribution)* is the step that maps faces—often by measuring the distance between the eyes, the shape of the chin, the distance between the nose and mouth—and then converts that into a string of numbers or points, often called a "faceprint." Goofy Instagram or Snapchat filters use similar technology (video). Although analysis can suffer from glitches, particularly involving misidentification, that's generally problematic only when the faceprint is added to a recognition database.
- *Recognition* is the attempt to confirm the identity of a person in a photo. This process is used for verification, such as in a security feature on a newer smartphone, or for identification, which attempts to answer the question "Who is in this picture?" And this is where the technology steps into the creepier side of things.

The detection phase of facial recognition starts with an algorithm that learns what a face is. Usually the creator of the algorithm does this by "training" it with photos of faces. If you cram in enough pictures to train the algorithm, over time it learns the difference between, say, a wall outlet and a face. Add another algorithm for analysis, and yet another for recognition, and you've got a recognition system.

The diversity of photos fed into the system has a profound effect on its accuracy during the analysis and recognition steps. For example, if the sample sets mostly include white men—as was the case in the training of early facial recognition systems—the programs will struggle to accurately identify BIPOC faces and women. The best facial recognition software has started to correct for this in recent years, but white males are still falsely matched less frequently (PDF) than other groups; some software misidentifies some Black and Asian people 100 times more often than white men. Mutale Nkonde, fellow of the Digital Civil Society Lab at Stanford and member of the TikTok Content Advisory Council, notes that even if the systems are operating perfectly, issues with gender identification remain: "Labels are typically binary: male, female. There is no way for that type of system to look at non-binary or even somebody who has transitioned."

Once a company trains its software to detect and recognize faces, the software can then find and compare them with other faces in a database. This is the *identification* step, where the software accesses a database of photos and cross-references to attempt to identify a person based on photos from a variety of sources, from mug shots to photos scraped off social networks. It then displays the results, usually ranking them by accuracy. These systems sound complicated, but with some technical skill, you can build a facial recognition system yourself with off-the-shelf software.

A brief history of facial recognition

The roots of facial recognition formed in the 1960s, when Woodrow Wilson Bledsoe developed a system of measurements to classify photos of faces. A new, unknown face could then be compared against the data points of previously entered photos. The system wasn't fast by modern standards, but it proved that the idea had merit. By 1967, interest from law enforcement was already creeping in, and such organizations appear to have funded Bledsoe's continued research—which was never published—into a matching program.

In 2001, law enforcement officials used facial recognition on crowds at Super Bowl XXXV.

Throughout the '70s, '80s, and '90s, new approaches with catchy names like the "Eigenface approach" (PDF) and "Fisherfaces" improved the technology's ability to locate a face and then identify features, paving the way for modern automated systems.

Facial recognition's first dramatic shift to the public stage in the US also brought on its first big controversy. In 2001, law enforcement officials used facial recognition on crowds at Super Bowl XXXV. Critics called it a violation of Fourth Amendment rights against unreasonable search and seizure. That year also saw the first widespread police use of the technology with a database operated by the Pinellas County Sheriff's Office, now one of the largest local databases in the country.

Skip ahead a few years to 2008, when Illinois's Biometric Information Privacy Act went into effect, becoming the first law of its kind in the US to regulate the unlawful collection and storage of biometric information, including photos of faces. Jennifer Lynch, surveillance litigation director at the Electronic Frontier Foundation, describes BIPA as the model for commercial regulation. "Illinois requires notice and written opt-in consent for the collection of any kind of biometric," she says. "At this point, Illinois is the only state that requires that."

The 2010s kickstarted the modern era of facial recognition, as computers were finally powerful enough to train the neural networks required to make facial recognition a standard feature. In 2011, facial recognition served to confirm the identity of Osama bin Laden. In 2014, Facebook publicly revealed its DeepFace photo-tagging software, the same year facial recognition played a key part in convicting a thief in Chicago and the same year Edward Snowden released documents showing the extent to which the US government was collecting images to build a database. In 2015, Baltimore police used facial recognition to identify participants in protests that arose after Freddie Gray was killed by a spinal injury suffered in a police van.

Clearview AI made news in early 2020 when The New York Times revealed that the company regularly ran its recognition software against a database of photos scraped from sources across the internet, including social media, news sites, and employment sites.

Facial recognition first trickled into personal devices as a security feature with Windows Hello and Android's Trusted Face in 2015, and then with the introduction of the iPhone X and Face ID in 2017.

Things have ramped up since then:

- In 2017, President Donald Trump issued an executive order expediting facial recognition usage at US borders (and private airlines have since made their own efforts to incorporate the technology).
- In 2018, Taylor Swift's security team used facial recognition to identify stalkers, and China rapidly increased its usage. Facial recognition came to Madison Square Garden as a general security measure, and retailers in the US experimented with the tech to track both legitimate shoppers and shoplifters.
- In 2019, a landlord in New York tried installing it to replace keys, and several schools attempted the same.
- Today, a handful of cities—San Francisco, Oakland, and Berkeley in California, plus Boston and Somerville in Massachusetts—have banned facial recognition usage by government entities. The country has also seen the first known case of a false positive leading to an arrest in the US. After Black Lives Matter police-brutality protests started in June, several large facial recognition vendors, including Amazon, IBM, and Microsoft, put a halt on selling their technology to law enforcement.

However, other, new players have entered the arena. Clearview AI made news in early 2020 when The New York Times revealed that the company regularly ran its recognition software against a database of photos scraped from sources across the internet, including social media, news sites, and employment sites—which Wirecutter, and many others, were able to confirm with testing—in a process that it used to identify suspects. In May 2020, the ACLU announced a lawsuit against Clearview AI in Illinois state court alleging that it violated the privacy rights of Illinois residents under BIPA. Clearview AI is an outlier only in that it has faced public scrutiny: Equally less ethical software companies exist—companies that will sell their software to local law enforcement, usually with no oversight or public scrutiny into where the photos come from or how the identification algorithms work.

The arguments for and against facial recognition

Proponents of facial recognition suggest that the software is useful because alongside identifying suspects, it can monitor known criminals and help identify child victims of abuse. In crowds, it could monitor for suspects at large events and increase security at airports or border crossings. The most long-running type of facial recognition software runs a photo through a government-controlled database, such as the FBI's database of over 400 million photos, which includes driver's licenses from some states, to identify a suspect. Local police departments use a variety of facial recognition software, often purchased from private companies.

There's a long list of benefits facial recognition can offer outside of law enforcement, adding convenience or security to everyday things and experiences. Facial recognition is helpful for organizing photos, useful in securing devices like laptops and phones, and beneficial in assisting blind and low-vision communities. It can be a more secure option for entry into places of business, fraud protection at ATMs, event registration, or logging in to online accounts. Advertising and commercial applications of facial recognition promise a wide array of supposed benefits, including tracking customer behavior in a store to personalize ads online.

Brenda Leong, senior counsel and director of artificial intelligence and ethics at Future of Privacy Forum, suggested in an interview that proponents point to facial recognition as a replacement for loyalty programs or gated access: "You just walk through a set of cameras and all those things happen very seamlessly, sports arenas, event venues, amusement parks, all those places either are using or would have ideas of ways to use it similarly."

Facial recognition is helpful for organizing photos, useful in securing devices like laptops and phones, and beneficial in assisting blind and low-vision communities.

Opponents don't think these benefits are worth the privacy risks, nor do they trust the systems or the people running them. The first point of contention lies in the act of collection itself—it's very easy for law enforcement to collect photos but nearly impossible for the public to avoid having their images taken. Mug shots, for example, happen upon arrest but before conviction. Error rates in recognition are also problematic, both in a false-positive sense, where an innocent person is falsely identified, and a false-negative sense, where a guilty person isn't identified.

The facial recognition software that law enforcement agencies use isn't currently available for public audit, and the algorithms that power the detection and identification software are often closed-box proprietary systems that researchers can't investigate. When the public doesn't know how these facial recognition systems work or how accurate they are, the public doesn't know whether these systems are being used appropriately, especially in law enforcement. Joseph Flores, a software developer who in his free time uses machine learning for art projects (disclosure: I've worked on related artistic projects with Flores, for fun, not for profit), explained to me how he often intentionally biases his data sets to produce the results he wants, something law enforcement could also do: "You could do the same with your law enforcement facial recognition data to make sure that your friends were unrecognizable and your enemies were misidentified as criminals." Flores adds, "It's hard to challenge the legality or the reliability of math that you can't review. Especially with the data scale we're talking about. With no review everything is falsifiable and just modern phrenology."

The public doesn't know whether these facial recognition systems are being used appropriately, especially in law enforcement.

Another growing issue is law enforcement's interest in real-time recognition in live video feeds or police body-cam footage. But even cities that enthusiastically moved forward with the technology, such as Orlando, Florida—where the police department used Amazon's Rekognition software to attempt to identify suspects in real time from video streams—have dialed those efforts back after the technology failed to live up to expectations. But just because real-time facial recognition still suffers from hiccups on a large scale in live testing doesn't mean it won't become widespread in the future. The idea is so appalling to some communities that the practice is already temporarily banned in California, Oregon, and New Hampshire.

The future of facial recognition and regulation

Generally speaking, the future of facial recognition can take any of three possible forms: no regulation at all, some regulation, and banning.

No regulation

The *Black Mirror* episodes illustrating a world devoid of facial recognition regulation write themselves. Brenda Leong provided a few examples: "It's very easy to create very Orwellian futures, where things are tracking you everywhere you go by your face because cameras are everywhere. If you're a student it could be literally watching whether you're focusing on your work versus daydreaming. If you're an employee, monitoring your engagement on your computer or telling whether you wandered off somewhere else." The list of surveillance possibilities is nearly endless, with China's "Social Credit Score" or the London police force's use of facial recognition cameras in real time offering a glimpse of one particularly grim reality.

Regulation

As of this writing, there's one proposed US law on a federal level banning police and FBI use of facial recognition, as well as another that allows exceptions with a warrant. Still another bill requires businesses to ask consent before using facial recognition software publicly, and yet another bans its use in public housing. Although facial recognition is certainly having a moment, it's still unclear which of these bills, if any, will have enough support to become laws.

When anyone talks about regulating facial recognition, they need to divide the idea into two parts: regulating commercial use and regulating government use, including that of law enforcement.

For commercial use, Leong stresses, the main thrust of regulation concerning any commercial feature—a loyalty program, theme park VIP access, or whatever else—should be consent. Facial recognition "should never be the default," she says. "It should never be part of the standard terms of service or privacy policy. And it should never be like the thing that happens that you have to then go opt out of." The easiest way to see how such

regulation might work in practice on a federal level is to look at Illinois's BIPA, which requires consent before an entity can collect and use biometric data (including faceprints) and imposes requirements upon the storage of that data.

The list of surveillance possibilities is nearly endless

Consent can be tricky, though. It's one thing for a store to ask if you want to skip showing your ID to enter and another when the store uses this technology to track shoplifters across all its franchise locations. As an example, the EFF's Jennifer Lynch points to a recent case of a business district in London where a company placed cameras in a privately run area that people who worked nearby passed through: "You could see that the business district might say, 'Oh, well, we put up signs,'" Lynch says. "And so people know that when they walk in this area or their face is being recorded and captured, but I don't really believe that people can actually meaningfully consent in that situation. If you are working in that area, you may not have a choice of working somewhere else."

When it comes to the government's use of facial recognition, suggested policy approaches diverge. Leong says that although Future of Privacy Forum's main focus is on commercial use of facial recognition, the group would want to see regulation of government use, too. "We would very much like to see overt, intentional regulatory guidance around how the government can and should use facial recognition," she says, "even if it's just things like being really clear about what levels of warrant or probable cause are required for agencies to access it."

Other groups, including the EFF, don't think regulation of law enforcement can go far enough.

Banning

Lynch, along with the EFF, argues that regulation isn't sufficient. "We are pushing for a ban or at least a moratorium at the federal, state, and local level on government use of face recognition," Lynch says. "It is a really game-changing technology and I think we're at a key point in history where we could prevent broad government use of face recognition."

Even as facial recognition addresses its diversity problem, there are still too many potential issues concerning how it's used. "The security and policing industries are predicated on this idea that Black people are dangerous," Mutale Nkonde says. "And so when thinking about tools for policing or tools for security, there is going to be this disproportionate deployment against Black people." That is why Nkonde supports banning the software's use outright: "I would want to see a ban around human subjects, just because I think the privacy trade-offs are too huge."

Privacy tips for using everyday things with facial recognition

Although policy changes, whether in the form of regulation or bans, offer the clearest way forward on a national scale, enacting such changes takes time. Meanwhile, there are smaller but not insignificant ways people interact with facial recognition on a daily basis that are worth thinking deeply about.

“I think that the concerning thing and the place where the distinctions sort of blur is that the more we use face recognition, the less we start to think of it, the less we think of it as risky out in the world, we become accustomed to it,” says Lynch. “I think it’s a slippery slope from using face recognition on your phone to the government using face recognition to track us wherever we go.”

- **What about facial recognition in Google Photos or Apple Photos?** Photo organization was the first time many people saw facial recognition in action. Apple has made a big show of describing how its facial recognition data in Photos runs on the device (PDF). This technology is more private than a cloud server, but it is also less accurate than cloud-based software. Face grouping in Google Photos can be very accurate, but Google’s wide array of services and devices means the company tends to share data liberally across the services it provides. In 2016, Google was sued in Illinois for its use of facial recognition, but that suit was later dismissed. In 2020, a new class action suit alleges a similar offense. Although the ability to organize photos by faces using the facial recognition feature in a photos app offers quantifiable benefits, there is a privacy trade-off to consider. It’s difficult to know exactly how a company might misuse your data; this was the case with the photo storage company Ever, whose customers trained the Ever AI algorithm without realizing it. You can disable face grouping in Google Photos. You can’t turn the corresponding feature off in Apple’s Photos app, but if you don’t actively go in and link a photo to a name, the recognition data never leaves your device.
- **What about Facebook?** Facebook likely has the largest facial data set ever assembled, and if Facebook has proven anything over the years, it’s that people shouldn’t trust the company to do the right thing with the data it collects. Facebook recently agreed to pay $550 million to settle a lawsuit in Illinois over its photo tagging system. Here’s how to opt out.
- **What about unlocking a phone or computer?** As the features work now, face unlock typically happens only on the device itself, and that data is never uploaded to a server or added to a database.
- **What about facial recognition in home security cameras?** The systems behind security cameras lack clear consent as they record and opt-in people automatically, often in defiance of local privacy laws, an ethical problem many people neglect to consider. Right now, only a handful of home security cameras include facial recognition, including Wirecutter’s smart doorbell upgrade pick, Google’s Nest Hello. Face detection on Nest cameras is off by default, however. More worrisome to privacy advocates is the potential inclusion of facial recognition with Ring cameras, a system that shares data with police through its Neighbors app.

- **Do you need to worry about those goofy face apps that pop up once a year or so?** The most recent app to break through in this arena was FaceApp, which gained popularity by allowing people to age themselves. Although the company says it doesn't use the app to train facial recognition software, it's difficult to know what might happen with the data the app collects if the company gets sold. The same goes for whatever the next version of FaceApp is. It's best to be wary of this type of software.
- **Can facial recognition identify you if you're wearing a mask?** It's not likely right now but may be in the future. One company in China was able to get facial recognition working on 95% of mask wearers, but this specific software was designed for small-scale databases of around 50,000 employees. Companies are scrambling to solve this problem.

Where society goes from here promises to be a mixture of policy and tweaks to people's personal habits, but the conversation concerning the technology likely isn't going anywhere for a long time. Like any technology, facial recognition is itself just software, but as Mutale Nkonde notes, how society uses it is what matters: "It's the way the tool impacts our civil and human rights that is my point of intervention, because I think that all technology is agnostic."