us.norton.com

What is facial recognition and how does it work? - Norton

Clare Stouffer July 21, 2023 3 min read

15–19 minutes

---

1. Blog Home
2. Internet Of Things
3. What is facial recognition and how does it work?

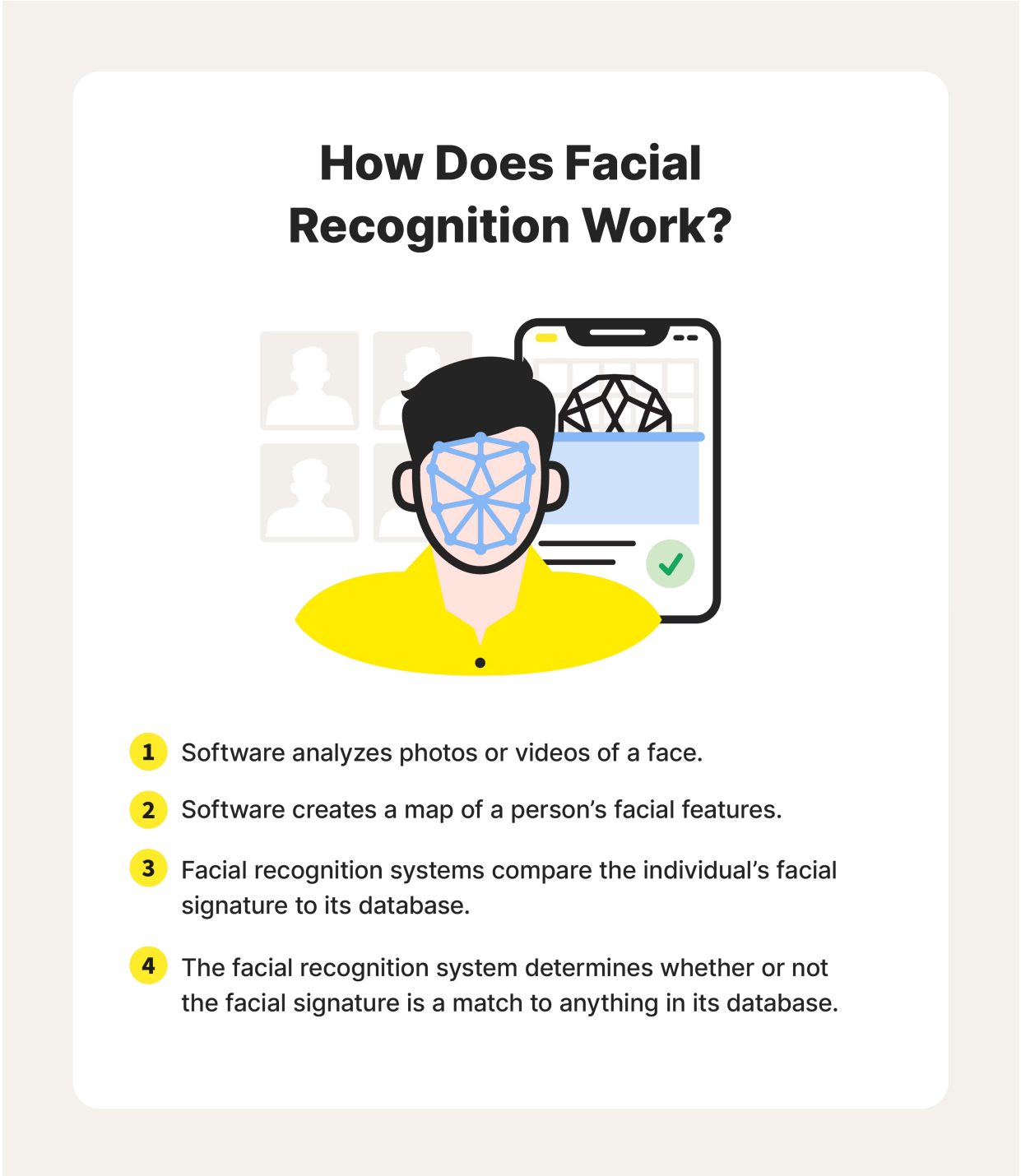
If privacy is important to you, you probably want some control over how your personal information and data get used. And here's the thing: Your "faceprint" is data. Although legislation is a bit behind in allowing individuals to protect their faces from AI, there are other ways to keep your personal information secure. Reading this guide is a start, but also note that Norton 360 Deluxe includes a password manager and dark web monitoring to help protect your personal information and alert you when it falls into the wrong hands.

Facial recognition is a way of identifying a human face through technology known as biometrics, oftentimes mapping facial features from a photograph or video and then comparing the information with a database of known faces to find a match.

And from the phone in your pocket to the cameras at your favorite concert venue, facial recognition is everywhere—and the facial

recognition market is only growing. It's expected to reach $16.74 billion by 2030, an increase of over 125% compared to valuation in 2020. Dive into this guide to learn more about facial recognition and how to interact with it safely.

How facial recognition works



Facial recognition uses technology and biometrics — typically through AI — to identify human faces. It maps facial features from a photograph or video and then compares the information with a database of known faces to find a match. Facial recognition can help verify a person's identity but also raises privacy issues. This is how it works:

1. Software is presented with at least one video or image that shows an individual's face.
2. Software scans videos and images to create a map of a person's facial features called a facial signature. This includes data like their eyes' precise location, scars, or other facial differences.
3. Facial recognition systems compare the individual's facial signature to its database. Today, many databases contain tens of millions to billions of images.
4. The facial recognition system determines whether or not the facial signature is a match to anything in its database. Some systems may also calculate an accuracy score or provide alternatives.

You can probably identify the face of a family member, friend, or acquaintance in a cinch. Without really thinking about it, you're familiar with their facial features — their eyes, nose, mouth, and how they come together.

Facial recognition systems also recognize those features — they just use an algorithm instead of a brain to put it together and identify a person. Where you see a face, recognition technology sees data. That data can be stored and accessed.

A Georgetown University study found that half of all American adults have their images stored in one or more facial recognition

databases that law enforcement agencies can search. This number has undoubtedly grown with the use of facial recognition in cell phones and with companies like Clearview AI scraping social media to train algorithms. The Internet of Things — referring to the many internet-connected devices we surround ourselves with — means facial recognition technology will likely keep growing.

Where facial recognition is used

Facial recognition systems are already being used all around us, from the phone in your pocket to the security cameras you pass while grocery shopping. Here are some common places you'll find facial recognition hard at work, making your life easier:

- **At airports:** The Department of Homeland Security has used the technology to identify people who have overstayed their visas or may be under criminal investigation. Some airlines will also scan faces at departure gates. Passengers flying British Airways can verify their identity via facial scan to board without scanning their passports.
- **In cellphones:** Apple first used facial recognition to unlock its iPhone X and access your digital wallet. The company has continued using facial recognition in new models. Apple says the chance of a random face unlocking your phone is about one in 1 million.
- **In the classroom:** Facial recognition software is being rolled out nationwide to improve security and monitor who's on campus.
- **On social media:** Facebook uses an algorithm to spot faces when you upload a photo to its platform. The social media company asks

if you want to tag people in your photos. If you say yes, it creates a link to their profiles. Facebook can recognize faces with 98 percent accuracy.

- **In businesses:** Some companies have traded in security badges for facial recognition systems. Retailers can combine surveillance cameras and facial recognition to scan shoppers' faces and identify potential shoplifters.
- **Marketers and advertisers in campaigns.** Marketers often consider gender, age, and ethnicity when targeting groups for a product or idea. Marketers can use facial recognition to define those audiences at stores or events

Facial recognition pros

As a relatively new technology, we're still understanding the pros and cons of facial recognition for everyday people. Here are some of the main advantages:

- **Fly safer:** Airports use facial recognition to identify criminals or potential threats.
- **Identify criminals:** Facial recognition can identify suspects from photos or videos.
- **Find missing persons:** Missing persons have been identified using facial recognition technology.
- **Keep your phone secure:** Many phones today use facial recognition to unlock or verify your identity before purchasing.

Facial recognition cons

It's important to understand the limits of facial recognition AI. For example, Randal Reid was arrested and jailed for a week in 2022 after being falsely identified by facial recognition technology. He had never even been to Louisiana, where the crime occurred.

Here are some of the top disadvantages of facial recognition:

- **Mistaken identity:** Relying on facial recognition alone can lead to falsely identifying criminal suspects.
- **Inaccuracies with older adults:** Facial recognition becomes less accurate when people age.
- **Racial and gender bias:** Studies have shown that facial recognition is less effective in identifying people of color and women.
- **It can be tricked:** Wearing a mask, sunglasses, or even certain makeup can make facial recognition less accurate.
- **It can violate privacy:** Many critics worry that facial recognition is one more erosion of personal privacy. With more accurate algorithms, it's becoming more of a risk that someone can take a photo of you in public and use AI to find more information.
- **It poses security risks:** Your facial data can be collected and stored, often without your permission. Hackers could access and steal that data.
- **There are potential ownership issues:** You may have given up your right to ownership over images of your face when you agreed to social media privacy policies.

Cybersecurity tips for using facial recognition

Privacy matters. People want the ability to control their personal information and how companies use it — including faceprints.

Want to protect your privacy in a world where facial recognition technology is becoming more common? Here are some reasons for hope:

- **Use facial recognition blocking glasses:** These can offer some protection against facial recognition AI but may not be as effective against more complex algorithms.

- **Opt out of social media facial recognition systems:** Social media platforms like Facebook have their own facial recognition systems. You can opt-out in your settings.
- **Secure your router:** With the Internet of Things, many devices in your home might have your facial scan, from gaming consoles to smart home devices. Ensure your router uses a firewall to keep everything safe.

Find more protection against facial recognition systems

Will hackers really want to steal your face? If they can use your facial data to commit fraud or turn a profit, the answer is “maybe.” Add that to the list of cyber safety risks. A holistic Cyber Safety package is worth considering to help protect your online privacy and security.

Still, facial recognition represents a challenge to your privacy. After all, there are few rules governing its use. Luckily, you can use Norton 360 Deluxe to help protect your data in other areas. With key features like password management and virus protection, your information and devices are better protected so you can browse more safely.

FAQs about facial recognition

Keep reading for our answers to your top questions about facial recognition.

Can facial recognition work with a mask?

The masks people wear during the COVID-19 pandemic pose challenges for facial recognition. But companies are working to overcome this by focusing their technology on the facial features visible above these masks. That could mean that a COVID mask, or other types of respirators and surgical masks, won't thwart facial recognition technology for long.

What is facial recognition used for?

Facial recognition has many uses. Companies can use it for marketing, sending targeted ads to consumers. Law enforcement agencies use it to identify suspects or track down missing persons. And tech companies use it to allow consumers to unlock their devices easily.

How accurate is facial recognition?

Some facial recognition technology companies boast accuracy rates of nearly 100%. According to the Center for Strategic & International Studies (CSI), facial recognition algorithms can hit accuracy scores as high as 99.97% on the National Institute of Standards and Technology's Facial Recognition Vendor Test when using clear reference images, such as from a passport.

In the real world, though, accuracy rates are usually lower. The Facial Recognition Vendor Test found that the error rate for one algorithm rose from 0.1% to 9.3% when reference photos were taken in public compared to using high-quality mugshots.

Aging is another challenge. According to the Face Recognition Vendor Test, better-quality algorithms can identify aging faces

more accurately. However, the results varied by a lot. Error rates ranged from 1.6% to 15.4% when searching for people whose photos in the database were 18 years old.

What are some examples of biometric technology?

Facial recognition, fingerprint analysis, voice recognition, DNA testing, and retinal scans are all examples of biometric identification technology you might be familiar with.

Is facial recognition technology safe?

Facial recognition has a lot of potential to make us safer by locating missing persons and identifying criminals. However, there are some concerns about data getting into the wrong hands. To keep yourself safe, take extra care to ensure that you're browsing securely, like using a VPN on any devices that have your face scan.

Can facial recognition be fooled by a photo?

Cybercriminals can fool phones with less sophisticated facial recognition capabilities with a photo. Only use facial recognition on devices that use 3D facial maps to ensure your information is safe.

What is face recognition on a phone?

Many smartphones now can use their cameras to scan your face. This scan can help you unlock your phone, log in to your accounts, and even make purchases without typing in your password.

- Clare Stouffer
- Gen employee

Clare Stouffer, a Gen employee, is a writer and editor for the company's blogs. She covers various topics in cybersecurity.

Contents