

How does face recognition feature destroy your privacy?

With the development at breakneck speed and too few control regulations today, does face recognition technologies put an end to personal privacy?

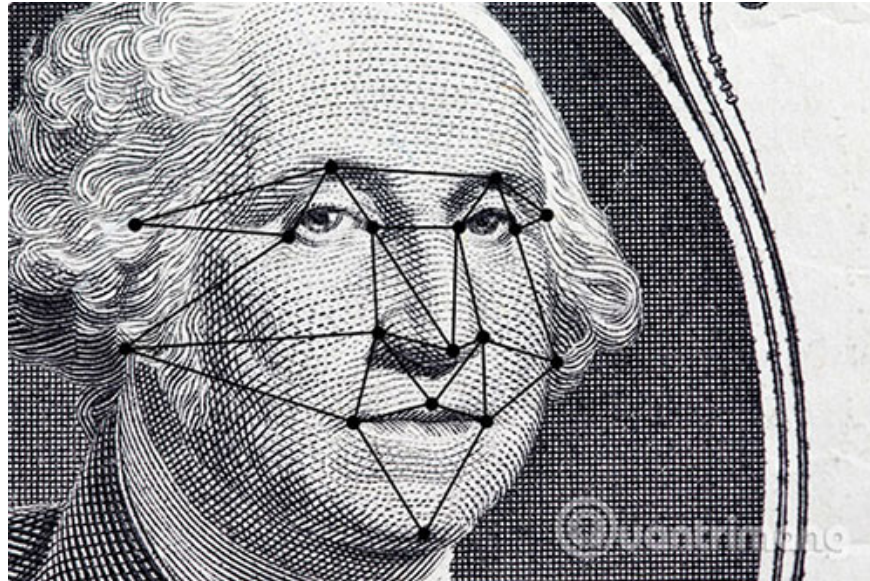
Face recognition technology has quickly shifted from being in science fiction movies to reality. Over the past few years, companies have been racing to release products with facial recognition features. Now, you can unlock your phone, board the plane and enter the house without touching your finger.

Law enforcement agencies around the world also quickly pursue the trend of face recognition and start implementing surveillance products. But, with the development of the dizzying speed and too few control regulations today, does face recognition technologies put an end to personal privacy?

Does face recognition technology put an end to privacy?

1. How does face detection work?
2. Take pictures and tag photos
3. Face recognition in business
4. Can you protect yourself from face recognition?

How does face detection work?



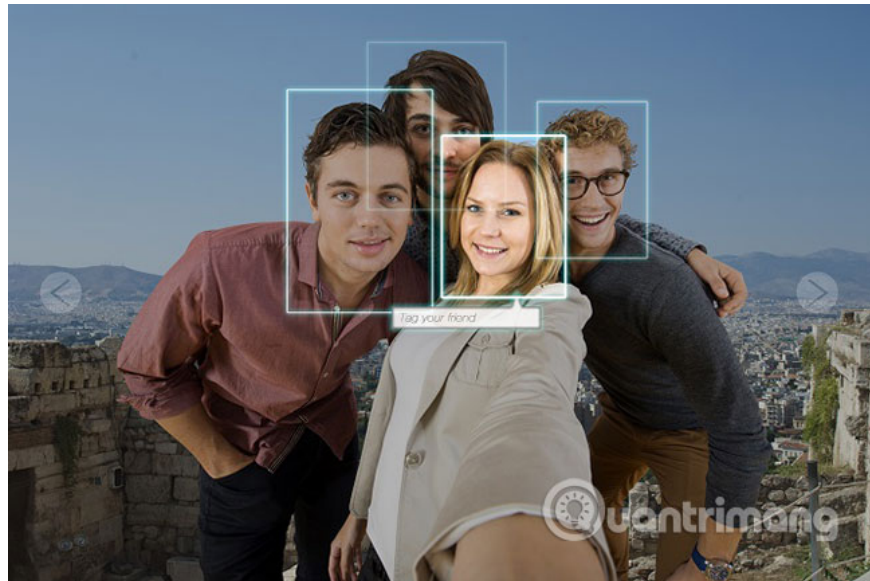
The presence of security cameras and video surveillance devices has been more popular than ever, since some of the first CCTV models were released in the mid-1990s. These cameras record events, helping detect and prosecute criminals and make many people feel safer.

In the decades when computer hardware and software improved rapidly. Next is the popularity of smartphones, which we use to capture and post millions of photos, as well as videos every day.

Face recognition system uses the abundance of this image data. Photos and videos are analyzed by software, often containing machine learning-related elements and artificial intelligence (AI). These algorithms search, analyze and store facial recognition information.

Just like the web browser can be used to identify you, so is the data about the face. This information is stored in the face recognition database and used to compare with new images and videos. These databases are often controversial because there is no way for you to get rid of them yourself. Databases can be operated by private companies or organizations.

Take pictures and tag photos



Facebook is one of the first sites to popularize the idea of tagging someone in a photo. In the early days, this was a manual process, in which you had to click through your photo and enter the name of each friend.

The company soon realized that they could do it on behalf of users automatically. Facebook has accumulated a large database of faces, tagged as specific individuals, and can be analyzed. Now, if you upload photos to Facebook, this social network will automatically suggest who is in the picture using Facebook's face recognition search feature.

Some people have seen this as a privacy invasion, because users are automatically subscribed to this feature. The EU even ruled that Facebook must turn this feature off in its member countries.

However, after EU deployed GDPR in 2018, Facebook turned it on again. If you don't like Facebook to recognize your face, you may want to see the privacy settings on Facebook that users should know.

Facebook is not the only big technology company that tests face recognition in your photos. Apple and Google both offer similar features in their cloud photo storage. However, one of the main differences is that Facebook identifies people in the image, and Google and Apple group similar faces together for you to assign names.

Face recognition in business

Amazon Rekognition

Easily add intelligent image and video analysis to your applications.

Get Started with Amazon Rekognition



Amazon Rekognition makes it easy to add image and video analysis to your applications. You just provide an image or video to the Rekognition API, and the service can identify the objects, people, text, scenes, and activities, as well as detect any inappropriate content. Amazon Rekognition also provides highly accurate facial analysis and facial recognition on images and video that you provide. You can detect, analyze, and compare faces for a wide variety of user verification, people counting, and public safety use cases.

Amazon Rekognition is based on the same proven, highly scalable, deep learning technology developed by Amazon's computer vision scientists to analyze billions of images and videos daily, and requires no machine learning expertise to use. Amazon Rekognition is a simple and easy to use API that can quickly analyze any image or video file stored in Amazon S3. Amazon Rekognition is always learning from new data, and we are continually adding new labels and facial recognition features to the service.



AWS re:Invent 2017 Introducing Amazon Rekognition (2:56)

Recently, face recognition has also begun to enter the offline life. The world's largest retailer, Amazon, has expanded to physical stores with the acquisition of Whole Food and Amazon Go groceries. Amazon Go stores do not have a counter, and although they depend on the camera, they do not use face recognition as reported.

The company developed a facial recognition product, dubbed the **Amazon Rekognition**. Amazon has filed an application for this product to law enforcement agencies in the United States and this has been discussed, as soon as Congress considers drafting regulations on the use of mold identification. face.

Civil liberties groups advocate strongly against the application of such a system. However, this job does not seem to work. At the time of the article, parliament rejected the abstinence using facial recognition and the Amazon board voted to continue selling Amazon Rekognition software. The lack of transparency makes Amazon on the list of companies that don't really care about users' security issues.

Face recognition is also being used even at live music venues. A face recognition system was applied during Taylor Swift's Rose Bowl concert in May 2018. According to Rolling Stone, a kiosk was set up, allowing fans to watch rehearsal recordings. of Swift, there is a face recognition camera hidden inside.

Each face was sent to the headquarters in Nashville. There, the face detection process was done, based on the data of known Taylor Swift followers. The straightforward use of this technology may have reduced its usefulness, but did not raise moral questions, stemming from the application of face recognition without informing The vast majority of fans are scanned.

Can you protect yourself from face recognition?

If stand alone, the face recognition system seems useful. In theory, they can help identify criminals, allowing users to log in constantly to their device and automatically organize photo collections. However, if there are no rules, they can contribute to undermining user privacy. The rapid pace of change in technology makes it difficult for management agencies to keep up.

Products that apply face recognition feature are often sold to users under a security cover. However, you may wonder if the current tradeoff is worth sacrificing your privacy.

If you don't want your face to be scanned anywhere, consider using one of these techniques to avoid face recognition online and in public.

You finished reading the article "**How does face recognition feature destroy your privacy?**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

