Your face belongs to us

The secretive start up dismantling your privacy

Kashmir Hill

Your face belongs to Us is based on 3 years of research.

Kashmir Hill is a New York Times award winning journalist. This is her first book.

Not so long ago, automatic face detection was something citizens associated with science fiction.

I first heard of Clearview when I was in a hospital room in Switzerland. They claimed that they could identify anybody with a snapshot of the face

Privacy, a difficult word to define, was best described in the Harvard law Review as “ the right to be left alone”

I could only contact John Good via linked in as his profile said he worked for Clearview.

I sent him a message, never got a response

Concerns about facial recognition had been building for decades. A small company with mysterious founders and a large data base is reality.

There was a belief as early as Darwin's time that faces could be measured, even criminality was a reflection of the face.

The American railroads developed a seven type face system for their ticket examiners.

Early railroad tickets in America has male-female; slim-medium-stout; young-middle aged-elderly; hair – light – dark etc. printed on the side of the ticket. If the description didn’t match the passenger, then the travel ticket examiner could offload the passenger from the train.

The early face detection algorithms were about identifying and predicting criminals.

In 2016 the China government wanted to give all its citizens a score - a rating that could affect every part of their life.

Later that year , a new Russian face recognition system Find face was in play.

This concept of facial recognition is something industry, government and computer scientists had been looking forward to.

In 1956, a group of brilliant mathematicians got together to think about machine language and how machines could mimic human beings

A new computer technique that compressed facial image and corporate funding were enablers to this concept.

The super bowl 2001 was the first time a facial recognition system had been used on a large scale to detect criminals and offenders.

Early face detection worked 90 % if photos were taken indoors as outdoor pictures had a sun shadow effect

facial recognition worked better for men vs women and for older people vs younger people.

Neural networks blew away all the other approaches to AI. Speech recognition, image recognition and facial recognition got better.

Smartcheckr gave way to a new company – Clearview AI.

At the end of 2018, Clearview had collected a billion faces from the internet. The silicon valley tech giants were afraid to build a facial recognition tool.

In 2009, Google introduced Goggles where you could search a person with a photo.

When people used it they found it cool but underwhelming

There were no laws in California on the use of biometrics but Google was worried.

Google mined messages from Gmail to generate relevant ads. Google launched Buzz an ill - fated social network which was fed with insights from G mail

Consumers have a ‘privacy paradox’ – they understand privacy but do not do enough to protect it.

When the internet first came to American homes, many people registered anonymously using fake names.

Facebook convinced people to part with their identities. Marketers loved Facebook because it had real data on people, and their preferences.

The technology and its creators grappled with two questions-

When is it fair for people to be recognized and

when should people have a right to anonymity?

Clearview sold three product lines in the early days :

Clearview AI search, a background checking tool

Clearview AI camera which would alert if a criminal entered a hotel or bank

Clearview AI check in, a building screening system that could verify people’s identities

Many investors turned down the opportunity to invest in Clearview

In December 2011, the federal trade commission called a number of tech executives for a conference titled “face facts”

They warned Congress that danger loomed ahead with facial recognition technology.

In 2018, someone suggested to Clearview that they go and work with the New York Police Dept’s financial crimes wing which determines identity theft etc. That was a game changer.

Police officers wanted this technology not to make an immediate arrest but match as an ‘investigative lead”

Clearview was next used by the Joint Terrorism task force who found the app very useful.

In 2019, the department of homeland security solved a sexual abuse case of a young girl using Clearview technology and after that they were a big customer.

Facebook bought an Israeli company face.com, Zuckerberg wanted facial recognition to go from one identification from 300 pictures to 1 in a million.

In January 2020 police arrested a man named Robert after a wrong facial match. I wrote an article on this titled “ wrongfully accused by an algorithm” for the New York Times.

In every early case of poor facial recognition matches, the people were black.

In 2020 Madison square garden tried out Clearview AI because it wanted a bunch of unwanted lawyers not to enter the stadium.

Clearview was investigated globally and was declared illegal in at least 6 countries and was subject to $ 70 million in fines. They all declared that Clearview needed consent from their citizens to use their pictures.

International regulatory agencies came to the conclusion that Clearview does mass surveillance.

Indian security forces also tried out Clearview.

David, a porn addict used facial recognition to track all porn stars to their roots. He did the same for all his Facebook women friends

In an Illinois court room, the lawyer argued that “ we are not arguing that Clearview cannot collect pictures from the net, we are not arguing that Clearview cannot match those photographs, we are arguing that they cannot use nonconsensual captured faceprints to do that.

Police and high end casinos in England were using facial recognition.

Casinos used it to give their top tier guests white glove service.

Clearview kept looking for positive use cases of facial recognition technology to tout to the public and to sway detractors.

One of the activists biggest argument against facial recognition is that it is racist and does not work well on some ethnic groups.