Dalton Scharff

Professor Quirin

CS 0590: Social Implications of Computing Technology

22 March 2017

Faux Freeware ‘Facezam’ Finds Facebook Friends from Furtive Photos

*The Telegraph*, a daily British newspaper, reported on March 14 about a new smartphone application which caused a bit of a stir in the technology world. This app, Facezam, claimed to be able to find the Facebook profiles of anyone who appeared in a photo. Facebook already implements this technology when uploading a picture to your profile, using its automatic tag suggestion feature, but will only try to tag people who your Facebook friends. Facezam took this a step farther, encouraging users to try it with anyone.

The app claimed to be able to match most photos with one of the 1.9 billion Facebook users in under 10 seconds, which sounded a little farfetched. Perhaps this is what lead to the revelation that the app, which had only been seen through advertisements, was only a viral marketing strategy and did not actually exist. Facebook made an official statement later regarding the commotion about the possibility of the app’s existence. The outlined purpose of Facezam was against the Facebook’s own terms of service and would be banned before ever becoming available on an app store. However, *The Telegraph* cited similar apps that do exist to perform facial recognition for users, but the databases of faces for these apps are far smaller, and therefore less accurate, than the entirety of photos on Facebook.

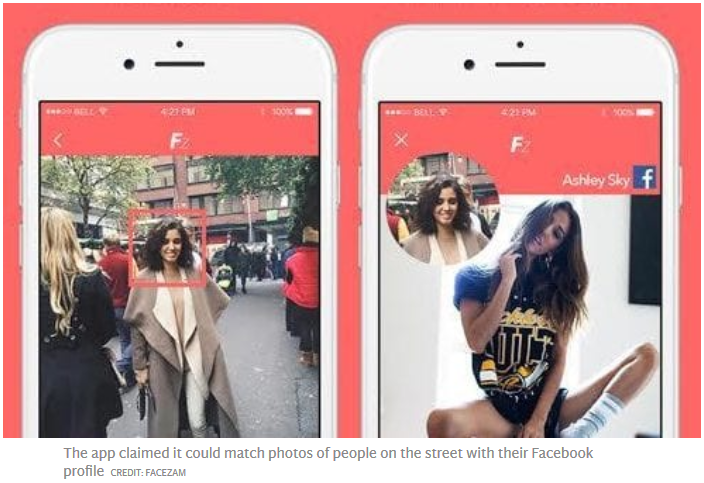
With the idea made publicly available, and prototypes already existing, it’s potentially only a matter of time before this gets made, either by someone illegally using Facebook as a database, or another large company compiling their own. The article talked about this technology as if it were the end of privacy all together. While it almost directly correlates to an episode of *Black Mirror*, which is known for its dystopian plots, I do not believe that this technology is necessarily bad.

While depending on your profile settings, most photos or videos uploaded to Facebook are considered private, where only Facebook friends can see them. Therefore, these should for no reason be used in a facial recognition database without the explicit consent of the uploader. However, profile photos can be seen by anyone, so does this make them fair game? I don’t believe so, because photography copyright laws state that whoever took the photo is that photo’s owner, unless otherwise stated in a legally binding agreement. It seems that Facebook wants to protect its user’s rights, so I don’t see the company turning this data over any time soon. Yet, government surveillance exists, especially in the United Kingdom, where *The Telegraph* is published. Getting arrested, running a red light, or simply walking on a sidewalk is enough to get your face in a government-recorded photograph or video. Although no paperwork was signed, the government has every right to record you since you are in a public place. Therefore, if the government is so inclined, and I bet it is, it could make its own database to scan against. The fiction you see in television shows like *CSI* just may become a reality.

While it feels like an invasion of privacy, this software could do good for the world. Imagine the possibilities of being able to identify criminals nearly instantly from a CCTV camera on a street corner. Of course, this technology could overstep its ethical boundaries, which is something we need to fight against. In the right hands and with the right regulations, though, facial recognition software like Facezam could make for a safer community.

# Facial recognition Facebook app hoax terrifies the internet

14 March 2017 • 10:13am

A fake facial recognition app that claimed to be able to identify strangers from a photograph has turned out to be a publicity stunt.

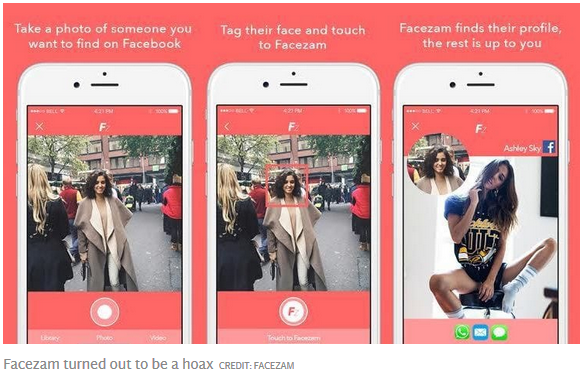
[Facezam](http://facezam.com/) claimed it could identify people by matching a photo of them with their Facebook profile. It was claimed that all users had to do is take a picture of someone on the street and run it through the app, which will tell them who it thinks the person in the photo is.

After the hoax was revealed to be the work of a viral marketing agency, Facebook said such an app violated its privacy policies.

"People trust us to protect their privacy and keep their information safe. This activity would violate our terms," Facebook said.

Facezam falsely claimed it could scan billions of Facebook profile images a second, through a database for developers, until it found a match. It claimed to be able to link most photos with a profile on the social network within 10 seconds.

"Facezam could be the end of our anonymous societies," said Jack Kenyon, who claimed to have founded Facezam. "Users will be able to identify anyone within a matter of seconds, which means privacy will no longer exist in public society."

Facebook reviews apps that use its data before they go live to check they [adhere to its policies](http://www.telegraph.co.uk/technology/2017/03/13/facebook-bans-companies-using-data-surveillance/). Apps that collect users' data or use automated technology to scan Facebook are forbidden from launching without permission from the social network.

The technology could help reduce crime by making everyone identifiable, Kenyon had claimed, adding that the public implications of the app couldn't be predicted. "There may be a mix of positives and negatives," he said.

### 'The end of anonymous society'

### 

The inspiration for the Facezam hoax comes from [Shazam, the music lookup service](http://www.telegraph.co.uk/technology/2016/09/29/shazam-reaches-profitability-as-it-hits-one-billion-downloads/) that can tell users the name and artist of a song after hearing just a few bars.

[Facial recognition software](http://www.telegraph.co.uk/technology/11693965/Facial-recognition-technology-Is-Orwells-fiction-our-reality.html) is already used by internet giants such as Facebook and Google to group photos together and suggest who should be tagged in them. It is also used in some law enforcement databases and by companies such as Tesco to map customer demographics.

Facebook [blocked the now defunct NameTag](http://www.prnewswire.com/news-releases/facialnetwork-releases-new-demo-of-facial-recognition-app-nametag-on-google-glass-receives-cease-and-desist-from-facebook-274649581.html), a Google Glass recognition app, from using its data in a similar way. [Google then banned the technology](http://www.telegraph.co.uk/technology/google/10095258/Google-Glass-bans-facial-recognition.html) altogether from being applied to Glass.

A [similar tool called Find Face](http://www.telegraph.co.uk/technology/2016/04/13/revealed-how-facial-recognition-can-open-up-your-life-to-strange/) lets users look up people online using a photo that it [matches with images on VKontakte](https://findface.ru/login), a Russian social network. British augmented reality company [Blippar recently launched a similar search tool](http://www.telegraph.co.uk/technology/2016/12/06/blippar-app-can-reveal-someones-identity-scanning-face/) but it can only scan faces on its database. These include public figures such as politicians and musicians, with users able to add their own faces if they want to.

**This story was updated after it was revealed to be a hoax.**

<http://www.telegraph.co.uk/technology/2017/03/14/creepy-facial-recognition-app-users-find-strangers-facebook/>