Dob by Mob and Facial Recognition

Shôn Ellerton, November 5, 2021

Smartphones and facial recognition could herald a scary new game called Dob by Mob.

Earlier this week, there was news of Facebook turning off its facial recognition system in response to allegations of misuse, namely those pertaining to privacy issues. I take this news as being welcoming but is it enough?

Few would disagree that Facebook has amassed too much information on our personal information; however, many forget that much of that personal information is willingly given, often unintentionally, without much thought of what happens to it when it reaches the other end. Where do all our posts, photos, videos and comments end up?

With a staggering 60 percent average of the population of the western world and 35 percent of the world's population on Facebook (according to statista.com), it may not come as some surprise that this $90 billion behemoth has grown from 370 million active daily active Facebook users in 2011 to nearly 2 billion in 2021. Considering this, the volume of data generated daily must be of gargantuan proportions necessitating the requirements of some very serious infrastructure. Much like other giant social media platforms, particularly that of YouTube, I still find it staggering when put into perspective. There is a fun website called everysecond.io which visualises the amount of how often something happens or is created each second, from how many Big Macs are sold to how many emails are sent. In the case of the Internet, the amount of data created each minute can be approximated to 1.7 terabytes and in the case of YouTube, something around the order of 60 minutes of video is uploaded each second.

That's a lot of data with a lot of faces that can be identified with increasing ease as artificial intelligence and data mining algorithms evolve! The worrying aspect is that one can never be sure if personal data uploaded to social media platforms are permanently deleted when requested. Although Facebook claims the facial recognition feature will be turned off for users, it does not necessarily entail that they don't have the means to identify faces.

That said, one could assume the 'safety in numbers' principle insofar that most of that data will eventually sink to the bottom of the vast unstructured data lakes to be forever lost in obscurity only to be resurrected when it gets re-discovered much like the proverbial silt on the bottom of a lake being disturbed. And sure enough, the vast majority of the data uploaded to Facebook is not of significant importance and left relatively undisturbed to eventually die from obscurity. But what of data which *is* of importance?

I recount in my earlier days working at T-Mobile in the UK, a mobile telecommunications company, as a design engineer. I was working on the HotSpot Wi-Fi network rollout and I was called in to the Public Affairs section of the building to provide enforcement agencies with confidential information for the purposes of tracking down a known criminal. This section of the building had been given an extra level of security with additional swipe card access. Apparently, as I understood, all mobile operators had a similar setup in which to provide police and enforcement agencies access to cell phone and Wi-Fi data records. I was the custodian of the system that tracked Wi-Fi logins through the network during that time; around 2004 or so. It came of no surprise then, that there was reason to doubt that any official or enforcement agency was given unfettered access to anyone's data. But this was during the days when facial recognition through data mining was in its infancy and not very effective. Roll on to 2019, and we can see what has happened in China and how advanced their facial recognition technology is.

Police *and* criminals or terrorists certainly use social media to their advantage. It is hypocritical of enforcement agencies when they state that social media and private messaging apps make it easier for terrorists and criminals to undertake their nefarious activities and should be more heavily controlled. It is often forgotten that the police and other enforcement or investigative agencies use this *same* technology to make it easier for *them* to coordinate activities to catch these criminals and terrorists! To suggest that criminals and terrorists don't monitor, analyse and process data on the web to avoid detection would be

terribly naïve. With facial recognition thrown in the mix, this massively augments the power of tracking and identifying picture tagged to a name.

I am aware of a worrying trend of dobbing against individuals on Facebook. For example, many police departments use Facebook to try to find the whereabouts of people who committed a crime, much like a modern version of a '*Wanted'* poster. I've noticed a trend in the increasing number of posts encompassing lesser and lesser crimes down to petty instances of unruly behaviour by a bunch of teenagers who happened to be drinking illegally in a public skate park at night. This, of course, attracts quite a commentary from the mob, much of it unhealthy and in the vein of vigilantism.

"Oh! They should be locked up!"

"They deserve a damned good thrashing!" (as John Cleese famously said in *Fawlty Towers*)

"Thank you for keeping us safe from those drunks!"

"Let's get a posse together and hunt them down like dogs!"

Posts of stolen cars is a common one with the police, and I have to confess that I found one amusing on all accounts. Someone had stolen a Bentley in an affluent eastern suburb of Adelaide. But it wasn't a nice Bentley that springs to mind, but rather one of those horrifically ugly Bentley Bentayga SUV cars. Judging by the commentary on the thread, it was aimed towards the *owner*, berating him (or her but doubt it) of having spent the best part of $600k on a car which looks like a piece of excrement.

On a more serious note, I am genuinely concerned about the advances made in facial technology, particularly so when it could be linked with other confidential data such as criminal and medical records. With the risk of confidential data being leaked, it is not unrealistic to suggest that in the not-to-distant future, the general public will be using their smartphones to scan people in crowds, much like the sport of fishing. Spotting someone who recently got fined would just be a mere minnow, catching someone who isn't vaccinated could be someone to dob on if the state mandated vaccines, and of course, spotting someone who was on the run for murder would be the big one, the marlin.

Worse still, the data could be intentionally released along with a reward. Forget all those nice little games like Pokemon Go, in which one walks around

‘capturing’ little imaginary creatures with a smartphone. The real thing will be walking around with a smartphone ‘capturing’ people who’ve done bad and naughty things.

The ultimate dobbing game for all the family to enjoy!