The Impact of Facial Recognition Technology on Society

Derek Benson

COMP 116: Information Security

December 13th, 2017

Abstract

No longer an academic dream or part of a science fiction novel, facial recognition technology is a reality that is just beginning to impact our everyday lives. This paper describes the history of facial recognition and examines questions like, 'is facial recognition technology a safe method for securing sensitive information?', and 'can facial recognition reliably be used to track individuals around an entire country?'. It also discusses some of the important legal ramifications that using facial recognition as a means of securing information can have.

Introduction

Facial recognition is the process of taking images or data of a face and associating that data with a specific individual. The technology has been portrayed for years in popular media. We've all seen shows where police were able to take grainy surveillance footage and run it through some sort of database to identify exactly who the perpetrator is. Throughout the 1990's and 2000's, despite an increasing number of commercial applications, popular media was where facial recognition stayed for the general consumer. As the technology progresses and evolves, new uses for facial recognition are being developed. These tools are now present in phones, video game consoles, and surveillance systems. As with most innovation, legislation lags significantly behind implementation. Yet, facial recognition tools are poised to have devastating effects on an individual's privacy and security throughout the world.

To the Community

Individual privacy in the United States has been taken for granted. For many years it was impractical for the federal government to spy on millions of people. However Snowden's revelations have shown the general public that the US government is now both capable of surveilling large segments of the population and willing to do it in secret. Now that facial recognition systems are able to produce near human-like accuracy, a large scale surveillance scheme run by the federal government based on facial recognition is much closer to reality. The TSA already announced and started implementing plans to use facial recognition and other biometric data to identify and track individuals, both citizens and foreigners, when they cross the United States border [8]. In China, a large scale surveillance program is already in place. It's slated to expand to almost 600 million cameras by 2020 and is capable tracking individuals as they go about their daily lives. When tested by a BBC reporter, it took authorities seven minutes to identify and locate him inside a large city using the system [11]. The Orwellian police state is no longer fiction. If you care about privacy then it's important that we call for legislation that regulates these kinds of systems before they are implemented without our input.

How facial recognition works

The origins of facial recognition date back to the 1960s. The early attempts were limited by processing power and some were only partially automated [3]. Engineers from Bell Labs tried to rely on features like, “ear protrusion, eyebrow weight or nose length, as the basis to recognize faces using pattern classification techniques” [3]. A Japanese researcher, Takeo Kanade, was able to successfully build the first fully automated facial recognition system in 1973. His system relied upon the same type of techniques as the Bell Labs research. First he digitized photographs, then they would be analyzed for specific facial features. Kanade was able to achieve up to seventy five percent accuracy on a specific collection of over eight hundred portraits [10]. These early methods were incredibly fragile. Just the introduction of a pair of glasses was enough to take Kanade’s system from a 75% identification rate all the way to less than 3% [10]. The 1980s saw the first attempts at using machine learning to solve the problem but it took until the 1990s for the first viable commercial applications of facial recognition to be developed [3]. The 1990s and 2000s saw an explosion of research and practical applications for facial recognition. Now facial recognition is everywhere. It’s in video game consoles, video conferencing applications, smartphones, surveillance networks, and social media.

Current facial recognition technology far surpasses the early attempts. Tech giants like Facebook and Google are applying machine learning algorithms to their massive databases of personal photos and information in order to build the next generation of tools. In 2014 Facebook published a research paper on ‘DeepFace’, a

facial recognition system that is able to score an accuracy of 97.35% over millions of photos [2]. Unlike earlier methodologies that focused on tagging specific facial features, Facebook's relies on the power of deep learning techniques to determine its own method of identifying individual faces given enough input to learn from. Identifying a face is normally broken down into a multistep process. The first subproblem is detecting the outline of a face in a photograph, then the face must be aligned to a standard portrait. Finally the face must be converted to some representation other than pixels and identified. Facebook's major improvements to this process were in the alignment and represent/identify steps [2]. To increase the accuracy of facial alignment, the researchers developed a way to extract a 3D model of the major facial features from the photo. Then they would rotate the 3D model and then convert it back to a 2D representation of the face so that the distortions caused by rotation didn't impact the placement of the points used to identify the face. Once the face was aligned, the raw pixels were dumped into a multilayered convolution neural network that extracted facial features and then identified the face [2]. One of the novelties of this style of approach is that specific facial features did not have to be manually tagged as focus points, given a large enough dataset of photographs the neural network was able to train itself which facial features to pay attention to and which ones to ignore. Given the incredible accuracy a system like this is now able to achieve, it's important to look at how this technology can be applied.

Facial Recognition and Privacy

Facial recognition technology has been worming its way into a surprising number of applications. Most recently Apple announced that facial recognition would be a key part of the iPhone X user experience. Despite all the fanfare, facial recognition has been in Android phones for over five years. While primarily a convenience feature, using your face to unlock your phone can have various security and legal implications. The original Android implementations had many questions related to their security. Clever individuals were able to beat these systems with digital photos or videos of the face that had been registered to unlock the device. In 2015, a researcher was able to take Alibaba's new mobile payment confirmation method by showing a video of his face to the camera[4]. The iPhone X's strategy for facial recognition takes a different approach that makes it immune to photo based attacks. Instead of taking a picture, an array of sensors makes an infrared 3D scan of the face looking at the device [5]. This method of scanning was supposed to be precise enough such that masks would have an incredibly difficult time fooling the system. It took slightly under a week for the Vietnam based security research firm Bkav to demonstrate a reproducible method of fooling the iPhone X's Face ID using a $200 mask [9]. Despite being marketed as a secure system, relying solely on Face ID to protect sensitive data is a mistake. Aside from the technical approach to cracking devices secured using biometric means like facial recognition, these biometric logins can make it remarkably easier for unauthorized agents to access your device through force. If a device contains sensitive information that a malicious party wants to access,

holding someone's face in front of the device to unlock it during a robbery is a much easier task than kidnapping that person to interrogate them for an actual password. While the concept of being kidnapped for the information on your phone is probably far fetched, there's also the more realistic scenario where the information on your device is needed for a court case.

Surprisingly, the way that your device is secured can actually impact how law enforcement officials are able to gain access to the device. So far tech companies have refused to install backdoors in their products for agencies like the FBI, this means that in order to access encrypted data these agencies have to be given access from the owner of the device. The Fifth Amendment of the Bill of Rights protects US citizens from being forced to incriminate themselves, so the question becomes whether forcing someone to unlock their device is a form of self incrimination. In U.S. v Doe (2011), the 11th US Circuit Court of Appeals found that forcing someone to produce a password to data that they encrypted is a violation of the Fifth Amendment [12]. The case was a big win for digital privacy advocates, but more recent cases have made the line much less clear. In January of 2017, a district court in Minnesota found that, "compelling a criminal defendant to provide a fingerprint to unlock the defendant's cellphone does not violate the Fifth Amendment" [13]. Since the act of giving up a fingerprint is not considered testimony, devices secured with a fingerprint scanner can be accessed by law enforcement if necessary. Although no court cases have yet been decided involving facial recognition to unlock a phone, it is likely that it will be more closely compared to producing a fingerprint than producing a password.

This entire situation is subject to change if a case on this matter ever makes it to the Supreme Court, as of right now the only way to prevent law enforcement from using your device to incriminate you is to use a secure password without enabling the fingerprint scanner or face unlock.

While facial recognition might provide law enforcement with an easier way to legally access the devices of suspects, it is also providing new tools to help identify criminal suspects. In the aftermath of the 2013 Boston Marathon Bombings, the FBI put out a plea to the public asking for help identifying several grainy photographs of Tamerlan and Dzhokhar Tsarnaev. The release of these photographs resulted in the successful identification of the brothers from their Aunt, but it also alerted the brothers that the FBI was on to them [1]. In a case study done after the incident, researchers attempted to apply several of the top facial recognition programs to the images released by the FBI. After experimenting with several of the software suites they were able to correctly identify Dzhokhar Tsarnaev based off of a publically available Facebook profile photo [1]. The technology has only improved in the four years since the Boston Bombing, and the potential for the identification of suspects using facial recognition looks promising. This promising nature has spurred the development of how governments can use facial recognition to not only identify criminals after the fact, but track and keep tabs on any potential criminals as well. The problem with deciding to preemptively track potential criminals is that it throws the concept of ‘innocent until proven guilty’ out the window. Is an algorithm deciding that

someone might commit a crime enough cause to warrant warnings and increased surveillance anywhere that person travels? China seems to think so.

For the entirety of human history, no government has had the means to successfully track and keep detailed records of the daily lives of all its citizens. It was always too time and resource expensive, but now technology has advanced to the point where the system can be automated. The most advanced surveillance system currently operational is in China. Powered by 170 million cameras with 400 million more being installed over the next 3 years [11], China is hoping to be able to track citizens around the country with accuracy of almost 90% [6]. This push is directly related to the new 'social credit' system that is targeted to be operational by 2020. The Chinese government is looking to aggregate everything from criminal records, to education records, to spending habits, and possibly social media interactions to generate a number that reflects how good of a citizen that person is [14]. This number is already being talked about for things like determining interest rates on loans, job offers, and even matches on online dating sites. Due to the secret nature of China's government, accurate statistics can be difficult to find but numbers from 2010 suggest that China's murder rate per capita is ¼ of America's [15]. Although China is the country clearly pushing further ahead with this technology, citizens of the United States shouldn't ignore the issue.

Despite advertising itself as the leader of the free world, it's clear by now that agencies like the NSA are willing to do whatever they are able to get away with thanks to Snowden. Just recently the TSA announced that they were planning on expanding

current border control procedures to include facial recognition scans and biometrics on both US citizens and foreign travellers [8]. This program started out just collecting information on a voluntary subset of travellers that wanted to be able to go through security faster. The scariest part of this program's expansion is that no congressional approval was required. The TSA will be storing images of US citizens crossing borders, at airport or on land, for up to 15 years. Since the information is stored, the TSA can offer interested parties access to the data. So far these interested parties have mostly been other government agencies like the FBI, but commercial entities like airline carriers and ticketing companies have been granted access as well [8]. As a country we have to decide if it's in our best interests to allow the establishment of a national database of information like that. It's one thing for your personal information to be used to tailor ads or tag friends in photos that you upload. Allowing companies that determine health insurance premiums, your mortgage rates, and more detailed access to information collected by agencies like the TSA would give them the ability to discriminate against certain groups of people.

Action Items

As citizens that live in a democracy, it's important to fight for our rights and protect them from being infringed upon. The easiest ways to protect your privacy as an individual are to avoid posting personal information and images to sites like Facebook, and to vote in elections. Federal legislative actions on issues like facial recognition are likely years away without a major lobbying effort. Therefore it is also important for citizens who feel that these technologies are being abused to challenge

the abusers in a court of law. The ongoing case Licata v Facebook is a class action lawsuit against Facebook for infringing upon an Illinois law that protects biometric data [7]. If we want to prevent the United States from implementing a surveillance system like China, then court and legislative battles are a crucial part of success.

Conclusion

Over the last several decades facial recognition technology has gone from the realm of academic research to a tangible network of hundreds of millions of cameras. Facial recognition has proven itself as a tool that can be both convenient and scary depending on how it is employed. There are many new questions that have to be answered about how to integrate this new technology into modern society. Should the government be able implement a nationwide surveillance network? Ten years ago that question could have been dismissed as infeasible, yet China has already partially built a functioning system capable of doing exactly that. Citizens have to be educated that facial recognition technology has moved well out of the realm of science fiction and is poised to become one of the key technologies responsible for shaping their everyday lives.

Sources

1) "A Case Study on Unconstrained Facial Recognition Using the Boston Marathon Bombings Suspects." http://www.nec.com/en/global/solutions/safety/pdf/MSU_Case_Study_on_Face_Recognition.pdf
2) “DeepFace: Closing the Gap to Human-Level Performance in Face Verification” https://www.cv-foundation.org/openaccess/content_cvpr_2014/papers/Taigman_DeepFace_Closing_the_2014_CVPR_paper.pdf
3) “Face Recognition Algorithms” http://www.ehu.eus/ccwintco/uploads/e/eb/PFC-IonMarques.pdf
4) “Face Recognition Security, Even With A 'Blink Test,' Is Easy To Trick” https://www.popsci.com/its-not-hard-trick-facial-recognition-security
5) “How secure is the iPhone C’s Face ID? Here’s what we know” https://www.wired.com/story/iphone-x-faceid-security/
6) “China will track its citizens’ every move with a new facial recognition system” https://thenextweb.com/asia/2017/10/17/chinas-upcoming-facial-recognition-system-will-obliterate-privacy-for-its-1-3-billion-citizens/
7) “Facebook's Facial Recognition Violates Privacy, Suit Says” https://www.law360.com/articles/638799/facebook-s-facial-recognition-violates-privacy-suit-says
8) “TSA Plans to Use Face Recognition to Track Americans Through Airports” https://www.eff.org/deeplinks/2017/11/tsa-plans-use-face-recognition-track-americans-through-airports
9) “Bkav’s new mask beats Face ID in "twin way": Severity level raised, do not use Face ID in business transactions” http://www.bkav.com/d/top-news/-/view_content/content/103968/bkav%92s-new-mask-beats-face-id-in-twin-way-severity-level-raised-do-not-use-face-id-in-business-transactions
10) “Picture Processing System by Computer Complex and Recognition of Human Faces” https://www.ri.cmu.edu/publications/picture-processing-system-by-computer-complex-and-recognition-of-human-faces/
11) “In Your Face: China’s all-seeing state” http://www.bbc.com/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state
12) “U.S. v Doe (In re: Grand Jury Subpoena Duces Tecum Dated March 25, 2011)” https://www.eff.org/cases/us-v-doe-re-grand-jury-subpoena-duces-tecum-dated-march-25-2011

13)“STATE OF MINNESOTA IN COURT OF APPEALS A15-2075“
https://mn.gov/law-library-stat/archive/ctappub/2017/OPa152075-011717.pdf
14)“China 'social credit': Beijing sets up huge system”
http://www.bbc.com/news/world-asia-china-34592186
15)“Country vs country: China and United States compared: Crime stats”
http://www.nationmaster.com/country-info/compare/China/United-States/Crime#2010