Facial Recognition and Law Enforcement

OSU CS391 Writing Assignment I
Lyell Read, Oregon State University
readly@oregonstate.edu

FOREWORD

As this issue is cutting edge, this piece relies heavily on [2], a well documented and well sourced New York Times article. There is limited additional information available, as Clearview has been in stealth mode (a startup strategy), and is also secretive (by my own judgment and as evidenced by their website which is quite scarce).

ISSUE OVERVIEW

Very recently, law enforcement agencies have begun using public-domain-searching AI facial recognition to identify suspects. As this technology was described in a legal review requested by Clearview, “In the simplest terms, [AI facial recognition] acts as a search engine of publicly available images [...] similar to Google” [7]. For the past 20 years, agencies would need to use local or federal photo databases to identify subjects [1]. These databases reportedly did not have great success on blurry or otherwise non-ideal footage [1]. This all has changed recently, as the company Clearview has started contracting with between 200 [7] and 600 [2] agencies, leveraging more than 3 billion images scraped from public services like “Facebook, YouTube, Venmo and millions of other websites” [2] - many times more images than the FBI has access to (FBI searches between 411.9 [2, 3] and 640 million images [4]), according to Clearview’s promotional materials [2, 5]. The company responsible, Clearview, is a stealth mode startup [2]. To date, all of Clearview’s technology and data remains closed source, including the functioning of their software. During the investigation that the New York Times engaged in, Clearview demonstrated that they are able to track searches made using their software [2]. Concerns were also raised about secret police photos of suspects being uploaded to the Clearview servers, with no guarantees of safety [2, 6]. Clearview was founded by Hoan Ton-That and Richard Schwartz (the latter an ex-aid to ex-mayor of New York Rudolph Giuliani) [2]. The startup was funded in part by venture capitalist Peter Thiel, and a firm called Kirenaga Partners [2]. Also, there is evidence that suggests that facial recognition accuracy can vary by race and gender [8, 9].

UTILITARIANISM

With respect to utilitarianism, this technology seems both morally justified and morally wrong. It can be viewed as justified when considered in the way that Clearview advertises their technology. In the promotional notes on the Clearview website, they include three sentence long snippets all about the ongoing challenge of sexual abuse of minors [10]. This evidently states where Clearview stands on how they suspect their technology will or should be used - to fight all crimes, including the most heinous, like the ones they reference. To that end, Clearview presents a morally sound product, if we consider it through a utilitarian lens. This product, when used right, has between a 75% [6] to 98.6% [11] success rate at matching an image to other publicly available images. With this success rate, and the exclusivity with which Clearview is marketed [11, 10] and sold [2, 6] to law enforcement agencies, this technology has the potential to be used effectively to society’s benefit, fighting crimes. When this light is cast on it, and combined with the many testimonials provided in [5, 6, 11], Clearview seems to be a general benefit for society, and justified as far as utilitarianism is concerned - from cutting down on crime, to reducing the costly search for unidentified persons, this definitely benefits the law abiding majority of society. When phrased like that, Clearview seems to be a successful startup poised to capitalize on a new age of criminal investigations, and more importantly seems to be an ethical proposal. With good news frequently comes bad news. Clearview is no exception – their technology has significant downsides in terms of personal privacy (tangentially, Clearview is not illegal [7][1] - that may be because it is an unregulated, emerging technology, and law has not yet been formulated to restrict the use of facial recognition). The problems with Clearview's product span further than questions of legality. What Clearview has done by starting to market their product is break an unspoken "Taboo" [2] on facial recognition use by law enforcement. Many companies before Clearview (including giants like Google, Facebook [13]) have had the capability to release such technology, but have refrained [13]. This step towards accurate facial matching for the masses is a dangerous one, and is also a precursor to a publicly-available versions of this tech [2]. If publicly available, anyone would have the ability to search a photo of a face and get a name – abolishing any sense of privacy among those who value such anonymity. Further uses of Clearview (and reasons why other companies have restrained from publishing their versions) include the ability to monitor everyone's whereabouts using CCTV and other live camera feeds, all running Clearview (or a cheap knock-off thereof, now that the taboo is broken [2]). Why is this unethical, though? Four reasons – firstly, Clearview has been rolled out without barely any public notice. Where otherwise this technology would be widely publicized and regulated, Clearview faces no such press or regulation. Now, if you are a suspect for a crime with one of these 200-600 agencies, chances are you will have your image searched using Clearview. Secondly, Clearview's accuracy varies based on the race and gender of the subject [9]. Needless to say, this could lead to a higher 'further investigation', arrest or conviction rate among groups for whom Clearview (and AI facial recognition) are less accurate. Thirdly, Clearview pulls it's data from online services, where photos were posted without this kind of high tech software using them to identify you. This can be seen as unethical as instead of the intended purpose of these images (to share with friends and family, or as part of a blog or video …), these photos are being used to seed a database of images that could later be used to track you down. The last reason that Clearview could be considered a decrement to privacy is their closed source model. They run proprietary algorithms on secret data from police departments (and evidence has been shown that they can view the searches that are placed by law enforcement agencies [2]), as well as the storage of private, possibly secret photos of ongoing investigations on their personal servers where there are no assurances of safety. Therefore, looking at Clearview's use in law enforcement agencies across the country with a utilitarian slant, the decision about whether this technology is moral or not comes from your personal stance on which is more important – lower crime rates, or personal privacy. Given that objectively, lower crime rates make the majority safer, whereas privacy does not necessarily compromise one's safety, I surmise that according to utilitarianism, Clearview is how we should proceed, as it benefits the majority - I find it to be morally sound with respect to utilitarianism.

KANTIANISM

As opposed to utilitarian ethics, kantianism requires a different set of rules to be considered in order to determine the morality of doing something. Kantian ethics require that we answer two questions: Can I rationally will that everyone act as I propose to act, and does my action respect the goals of human beings rather than merely using them for my own purposes? Kant believed these questions to be synonymous, so with that in mind, the second question is the most easily applied to this issue. This question can be rephrased to be: Does this technology respect the goals of human beings, or does it use them for its own purposes? Given how Clearview works, the technology behind it clearly violates this rule for a few reasons. Firstly, Clearview does not respect the goals of the humans that posted the images to the internet - most images are there for professional

[1] Given my lack of knowledge of law, I referred to the document published by Clearview themselves. Though this may be a biased document, without a full legal investigation on my part, I can neither verify that this document is free of bias, or prove illegality in any field.

connections (LinkedIn), for social connections (Instagram, Facebook, Imgur, Reddit), or as part of their source of income (YouTube, Vimeo, Blogs). The goals of the people that posted these images was clearly not to seed a database of images that would later be crawled by an AI algorithm to identify suspects. Secondly, the object of Clearview is arguably self interested - their goal is to make money, like all companies. In that light, Clearview is using the human subjects for its own benefit, rather than with their primary goal being societal benefit. Based on this, Clearview is unethical when considered against Kantian ethics.

ACM CODE OF ETHICS

Within the ACM code of ethics, there are many individual rules. Each of these rules address specific niches within their section of ethics. In order to be completely ethical, a technology needs to be in accordance with all these rules - otherwise phrased: if there is one rule where Clearview does not comply, the technology will be considered unethical. The first instance of such rule where Clearview is not in accordance is rule 1.2: Avoid Harm"[12]. Here, Clearview falls short for two reasons — firstly, it inevitably causes harm to suspects that are convicted of the crime they were suspected of, but more importantly, it poses the risk of false accusation of a crime. In this case, the technology could have mismatched an innocent's face to the suspect's and they would be (at the very least) taken in for questioning. Secondly, Clearview's database consists of a bunch of photos from the internet that were not published with the intention of being used as such. This can be considered to be a breach of privacy, and arguably a harm to those whose images are in the database. Therefore, Clearview is not ethical with regards to the ACM code of ethics.

ISSUE FUTURE

We can only wait and see what happens to Clearview, and AI facial Recognition within law enforcement over time – provided proper legislation, this technology could be confined to only positive, non-privacy-compromising uses, but I find that hard to believe. In today's complex political climate, if one of the two sides (Republican, Democrat) chooses a side on an issue like this, the other will default to the opposite, and dig in their legal heels. This makes it so that no well formed legislation can pass, and therefore, I expect to see this technology take over soon, unregulated or at least weakly regulated as it is today. Instead of just one company providing this technology, many will crop up to take advantage of the lucrative market there is for such services. Competition in this market will bring the price of using such services to close to free (this is relatively simple software, and thus offering an application with ads on it would likely provide a viable business strategy). Unethical operators of such services will welcome bribes to keep your likenesses out of their database (so a search for your image returns no results). Once facial recognition becomes commonplace, we will see a rise in technologies such as those theorized by Clearview founder Mt. Ton-That – products that can "vet babysitters or [be used as] as an add-on feature for surveillance cameras [or a] tool for security guards in the lobbies of buildings or to help hotels greet guests by name"[2]. All these ideas sound great, and that's partially because Mr. Ton-That is one of the founders of Clearview. What he will not talk about are the negative uses – compromising investigators working in the field, use against the population of our country like what China plans to implement in the future [14, 15]. With all law enforcement, the government, and likely private companies using facial recognition, the world will turn into a society like that in *1984* or any other dystopian future. Selling data about a person's whereabouts will be a common practice, as anyone with a surveillance camera and a facial recognition algorithm can determine this information. Advertisers will purchase this data to display personalized ads, for example, turning time's square into a veritable scene from *Blade Runner*.

REFERENCES

[1] J. Valentino-devries, “How the Police Use Facial Recognition, and Where It Falls Short,” *The New York Times*, 12-Jan-2020. [Online]. Available: https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html. [Accessed: 24-Jan-2020].

[2] K. Hill, “The Secretive Company That Might End Privacy as We Know It,” *The New York Times*, 18-Jan-2020. [Online]. Available: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html. [Accessed: 24-Jan-2020].

[3] A new report the government watchdog agency released Wednesday gives an unprecedented look at the scale of the FBI's facial recognition programs., “FBI's face-recognition system searches 411 million photos, including driver's licenses,” *CNNMoney*, 16-Jun-2016. [Online]. Available: https://money.cnn.com/2016/06/16/technology/fbi-facial-recognition/index.html. [Accessed: 24-Jan-2020].

[4] N. S. Guliani, “The FBI Has Access to Over 640 Million Photos of Us Through Its Facial Recognition Database,” *American Civil Liberties Union*, 10-Jun-2019. [Online]. Available: https://www.aclu.org/blog/privacy-technology/surveillance-technologies/fbi-has-access-over-640-million-photos-us-through. [Accessed: 24-Jan-2020].

[5] B. Lipton, “Records on Clearview reveal new info on police use,” *MuckRock*, 18-Jan-2020. [Online]. Available: https://www.muckrock.com/news/archives/2020/jan/18/clearview-ai-facial-recogniton-records/. [Accessed: 24-Jan-2020].

[6] K. Hill, “Clearview: The company that might end privacy as we know it,” *The Economic Times*, 20-Jan-2020. [Online]. Available: https://economictimes.indiatimes.com/tech/internet/clearview-ai-the-company-that-might-end-privacy-as-we-know-it/articleshow/73392042.cms?from=mdr. [Accessed: 24-Jan-2020].

[7] P. D. Clement, “Kirkland & Ellis, LLP Memorandum: Legal Implications of Clearview Technology.” Chicago, Il, 14-Aug-2019.

[8] J. Fingas, “Law enforcement is using a facial recognition app with huge privacy issues,” *Engadget*, 18-Jan-2020. [Online]. Available: https://www.engadget.com/2020/01/18/law-enforcement-using-clearwater-ai-facial-recognition/. [Accessed: 24-Jan-2020].

[9] I. D. Raji and J. D. Buolamwini, “Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products,” Massachusetts Institute of Technology, 2019.

[10] “Clearview,” *Clearview*. [Online]. Available: https://clearview.ai/. [Accessed: 24-Jan-2020].

[11] Clearview, qtd. in [2]

[12] “The Code affirms an obligation of computing professionals to use their skills for the benefit of society.,” *Code of Ethics*. [Online]. Available: https://www.acm.org/code-of-ethics. [Accessed: 24-Jan-2020].

[13] Q. Wong, “Facebook built a facial recognition app for employees,” *CNET*, 22-Nov-2019. [Online]. Available: https://www.cnet.com/news/facebook-built-a-facial-recognition-app-for-employees/. [Accessed: 24-Jan-2020].

[14] “Social Credit System,” *Wikipedia*, 23-Jan-2020. [Online]. Available: https://en.wikipedia.org/wiki/Social_Credit_System. [Accessed: 24-Jan-2020].

[15] C. Campbell, “How China Is Using Big Data to Create a Social Credit Score,” *Time*, 14-Aug-2019. [Online]. Available: https://time.com/collection/davos-2019/5502592/china-social-credit-score/. [Accessed: 24-Jan-2020].