Facial Recognition and Law Enforcement

OSU CS391 Writing Assignment II
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).

Certain sections have been split up to facilitate better organizing this paper, so they may not match up well to the Canvas guide.

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]. Given these facts, the issues with this technology, which will be elaborated on later, are fourfold. Firstly, this 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, though Secondly, 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. Thirdly, further uses of Clearview (and reasons why other companies have

[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.

refrained 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]). Fourthly, 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. Fifthly, 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. Lastly, Clearview pulls it's data from online services, where photos were posted without this kind of high tech software using them to identify you.

VIRTUE ETHICS

Now that a baseline has been established regarding the technology of, and issues surrounding, Clearview, we can delve into examining whether this technology is morally acceptable or otherwise. The first theory of ethics this will be examined against is that of Virtue Ethics. Virtue Ethics emphasizes, as is made evident by the name, the virtues of the decision maker [16]. Specifically, an action taken is only deemed morally 'right' if said action is one that a virtuous person would take in the same scenario [17]. To apply this to Clearview, we must first define what the decision is. For the sake of this comparison, and given the notion of 'taboo' [2] discussed previously, the decision will be that of releasing (or green-lighting, or founding) Clearview as a company. This decision was primarily taken by Mr. Ton-That, the founder, when he decided to start the company, and begin developing, marketing and selling Clearview. To decide if this choice was morally justified, we must examine what a perfectly virtuous person would have done in that situation. The traditional list of virtues includes prudence, justice, fortitude or bravery and temperance [17]. To start examining these virtues individually, the virtue of prudence would strongly advise against the choice to start Clearview - given that larger, more developed (and arguably wiser) companies have not released the same technology you plan to release, prudence would state that you must spend more time perfecting this software. This would include ensuring that when it goes public, there are no reasons that anyone could complain about the technology or it's use. Further, this encompasses going through public disclosure, open sourcing your software (personally I weigh a 'black box' program as more dangerous than public access to software like Clearview), and spending years refining your software to perfection before releasing it. These are all things that Clearview has not extensively done, and which demonstrate that if a perfectly virtuous individual were to be posed this decision, they would refrain. The decision to start Clearview is morally justified with relation to the virtues of justice (it, when used right, does help society achieve justice), and bravery (starting a company in such a contested space takes bravery and fortitude). Where the decision to found Clearview falls down again 'virtually' is at the virtue of temperance. For many of the same reasons as it failed the test for prudence, the release of a product that has neither been evaluated (except for legality, [7]) or analyzed for proper function and construction shows lack of temperance. For that reason, we can conclude that a perfectly virtuous individual would not make the decision to start Clearview in light of it violating their virtues of prudence and temperance.

SOCIAL CONTRACT THEORY

As opposed to Virtue Ethics, Social Contract Theory supports the deployment and use of Clearview. Social Contract Theory revolves around the rules that are established in the social contract (one person's contract of sorts with the next), as well as inherent (unalienable) rights, and lastly the common good. The core 'theory' to Social Contract Theory, today mainly revolves around legality - the social contract is mostly the laws that govern inter-person and person-society interactions. To this point, we can safely conclude that Clearview is acceptable as far as the social contract, as Clearview themselves have performed a legal review [7]. With respect to inherent rights of an individual, this breakdown becomes slightly less clear. For the sake of this paper, we'll analogize these inherent rights to the basic human rights. In this sense, Clearview AI does not egregiously violate any human rights. In today's digital age, though, one might argue that

privacy should be an unalienable right, in which case, Clearview would be in the grey-zone for the way that it uses (abuses, maybe) publicly available content. Lastly, Clearview (provided the numbers that represent the success rates are correct) support the common good - not only can it help solve hard to solve crimes, but in doing so, it can also free up law enforcement resources which either reduces the cost of law enforcement on taxpayers (slightly, granted), or it allows the units that would otherwise be hunting down a suspect based on an image to perform other duties that can contribute to the social good. Therefore, with respect to Social Contract Theory, Clearview is morally justified.

OSU CODE OF ETHICS

The OSU Code of ethics itself presents a small list of guidelines to follow when conducting university affairs. Counted among these are clauses about "Honesty and Integrity", "Respect", "Stewardship and Compliance", and "Accountability and Responsibility" [18]. Despite passing Social Contract Theory's ethical analysis, Clearview fails the OSU Code of Ethics. The very first section in the Code of Ethics states that "[we must conduct] ourselves free of personal conflicts, self-dealing, [not] using resources for personal benefit or gain" [18]. Clearview could definitely be considered in violation of this clause, as not only are they profiting from their technology, but they are also violating the "personal conflicts" clause (as it could be in their best interest to leave their founders' images out of the app). Under the "Respect" clause, Clearview also fails, as their software has been shown not to demonstrate "impartiality" [9]. The issues with race/gender accuracy defined in [9] could also be extended to be a violation of the clause that states "[we must] refrain discriminating against [...] others" [18]. Moving down the list to the "Stewardship and Compliance" section, we find the most egregious violation of the code of ethics. This section states that "We utilize resources and information entrusted to our care in a wise, ethical, and prudent manner" [18] - this is obviously something that the media has concerns about Clearview's ability to accomplish [2]. Among others, the reported level at which Clearview can access confidential data that is stored on their servers (as seen in [2]) constitutes both an unwise, as well as (arguably) unethical utilization of information. On to the last section, about "Accountability and Responsibility", we must consider the Clearview algorithm. This algorithm, given its closed-source and black-box like nature, can not be accountable. Unless the public (whom this tool will be used against) can verify the functioning of this algorithm, and give input on how to make it more accurate, this tool will always have low accountability. Thus on all four subsections of the OSU Code of Ethics, Clearview fails ethically, therefore it fails ethically overall as well.

IEEE CODE OF ETHICS

The IEEE Code of Ethics states that its goal is to encourage "the highest ethical and professional conduct" [19] from members of the professional world in technology fields. Given that Clearview is a technology company, this code of ethics is quite applicable to them. Starting at the top of the IEEE Code of Ethics, the first clause is a mixed bag for Clearview - at the same time, Clearview is in compliance as they do essentially improve "the safety [...] of the public" [19]. However, they are not in compliance as a result of their closed source / black-box algorithm. Both this algorithm, and their operating methodology violate the part of this clause concerning "disclos[ing] factors that might endanger the public" [19]. Clearview also fails the second clause, in the same way that it failed the OSU Code of Ethics - there are evident conflicts of interests among the directors of Clearview: it would be in their best interest to keep their images (and those of relatives, ...) out of the database. Again, the ethicality of Clearview is placed in question when considered in the light of clauses 3 and 4. These state respectively that Clearview should "be honest and realistic in stating claims or estimates based on available data" and "[should] reject bribery in all its forms" [19]. The former of these statements comes into question when the accuracy of Clearview tech is reported by Clearview to be 98.6% [11] accurate, while news outlets report it to be more like 75% accurate [6]. Further, despite research presented in [9], Clearview makes no mention of racial/gender differences in result accuracy. Clearview also infringes on the second of these clauses as there would be a serious (and untraceable, using bitcoin paired with the closed

source nature of the program) incentive to accept bribes to scrub photos of paying individuals from the database. Clearview fails clause 8 (“to treat fairly all persons [...] and to not engage in discrimination” [19]) because of the research presented in [9]. Given the closed source nature of Clearview, it fails clause 5. Clauses 6, 7, 10 are not directly applicable to Clearview (and likely would not improve its ‘ethicality rating’ in the eyes of the IEEE Code of Ethics if they were). It fails clause 9, as if someone is (improperly or not) convicted, they will experience “injury” or damage to their “reputation”. In light of failing nearly every applicable category, Clearview is deemed completely unethical with respect to the IEEE Code of Ethics.

OSU VS IEEE USING VIRTUE ETHICS

When thinking about how Clearview fared against both the IEEE and OSU Codes of Ethics, it failed against both, miserably. To look further into why Clearview can be considered morally justified using some codes of ethics, but is considered unethical in the light of the professional codes of ethics, we can contrast the IEEE and OSU Codes both with relation to Virtue Ethics. Virtue Ethics asks the question: is my decision the same as that which a perfectly virtuous person would make? Firstly, the first 2 clauses of the OSU Code of Ethics (those representing “Honesty and Integrity” and “Respect”) are ethically acceptable in the frame of Virtue Ethics, as well as the corresponding clauses 3, 4, 8 of the IEEE Code of Ethics. Things fall apart for the OSU Code when considered through Virtue Ethics when we reach clause 3, “Stewardship & Compliance”. This clause can be considered questionable as it states that “we utilize resources and information entrusted to our care in a wise, ethical, and prudent manner in order to achieve our educational mission” [18]. It is not guaranteeable that a perfectly virtuous individual would adhere to OSU’s Educational Mission, or that this person would propagate the “information” provided to them, as they will likely be unsure of the accuracy of such information. Similarly, the Virtue Ethics are questionable for clauses 1 and 10 of the IEEE code - these clauses both recommend actions that could not be the same decision as a perfectly virtuous individual would take. The former, clause 1, states that one should “hold paramount the safety, health, and welfare of the public” [19] - while on the surface this may seem like a guarenteeably ethical statement, if the perfectly virtuous individual were to know that today’s wellbeing would cause greater harm tomorrow, this would not be the choice they would take. Similarly with clause 10, “[one should] assist colleagues and co-workers in their professional development” [19], this clause emphasizes a situation with the possibility of future misuse of the information that was learned through the “professional development”. In this case, the virtuous being would certainly decide against this. The remaining IEEE codes are supported clearly by Virtue Ethics, and so is code 4 of the OSU Code of Ethics.

Of the two codes of ethics, the IEEE Code of Ethics seems to me to be the most likely to bring up the best results for the largest number of people. This is because the OSU Code is centered on the individual, while the IEEE addresses technology companies. Why does this yield the greatest outcomes for the most? As time goes on, more and more technology will be used, and this technology will become more pervasive in human life. Rather than being able to create the most good through inspiring good behavior on the human level, the most good will come from being able to lead technology companies towards more ethical practices that will, in turn, benefit many people. For making ethical decisions at a personal level, though, the OSU code seems more appropriate. It is individual centered. In this case, the IEEE Code will be partially ignored by the user as some clauses are not applicable to the individual.

Neither code discusses enforcement. It would be hard to enforce either code, as the codes read as statements of opinion, and trying to convince people that these codes must be followed will be hard. Especially in the case of the OSU Code, if the target individual disagrees fundamentally with the OSU message/goals, they will reject the entire set of guidelines, and the effort will lose its worth.

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].

[18] “Oregon State University University Code of Ethics,” 18-Jul-2014. [Online]. Available: https://pacs.oregonstate.edu/procurement/announcement/osu-code-ethics. [Accessed: 08-Feb-2020].

[19] “IEEE Code of Ethics,” *IEEE*. [Online]. Available: https://www.ieee.org/about/corporate/governance/p7-8.html. [Accessed: 08-Feb-2020].