Clearview AI and its ethical implications

Introduction

Clearview AI is a facial recognition start-up founded by Hoan Ton-That and Richard Schwartz in 2017. The areas served are the United States and Canada, with its headquarters in Manhattan, New York City, U.S (Wikipedia 2020). This is a new research tool used by law enforcement agencies to identify perpetrators and victims of crimes. Using this technology, law enforcement can catch criminals and solve cold cases (Clearview AI, 2020). The start-up has claimed to identify a person based on a single photo, revealing their real name, general location, and other identifiers (Cimpanu 2020).

Background

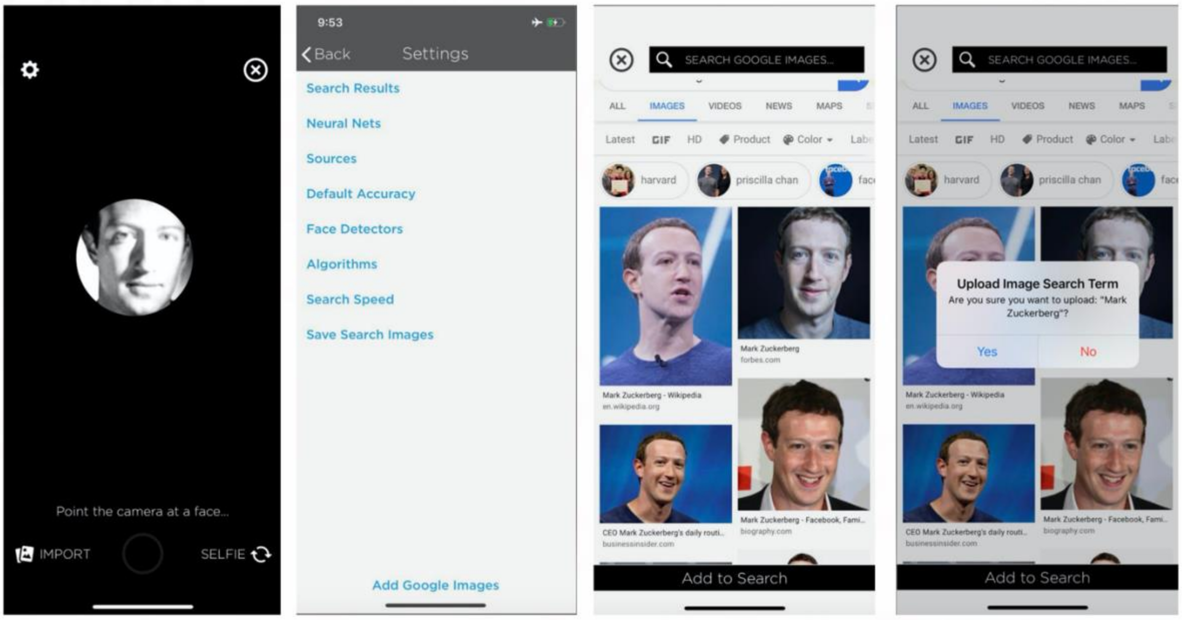
The three main reasons for the start-up were an increase in the sexual abuse imagery by 100x, Victims having a 25% higher risk of suicide, 78.3% of images show children under 12 (The expansion of the Internet has led to an explosion in the market for child pornography). It is used to help exonerate the innocent and identify the victims of the crimes, including child sex abuse and financial fraud (Clearview AI 2020).
Clearview database includes more than 3 billion images taken from the publicly available images from the web, including social media sites such as Facebook, YouTube. The tool works in this manner when you have an image of a person, but the name and details are unknown. The image can be uploaded into the app, and it returns the image of that person scrapped from the web and also the links to the websites from where the images came from. That is a fair amount of information to be available publicly. (Goldenfein 2020)

Potential ethical concerns

I. Privacy and security

- A chief security officer, Mossab Hussein from a cybersecurity firm, named SpiderSilk, had found the source code repository of Clearview AI. The security of Clearview AI was compromised as its server was misconfigured. Due to which anyone could register as a new user and login to the system. The repository consisted of the source code, company's secret keys, and the credentials with which cloud buckets could have been accessed. The storage buckets consisted of copies of its finished apps for Windows, Mac, and Android. It also consisted of the pre-release developer app version, which is meant only for testing purposes.

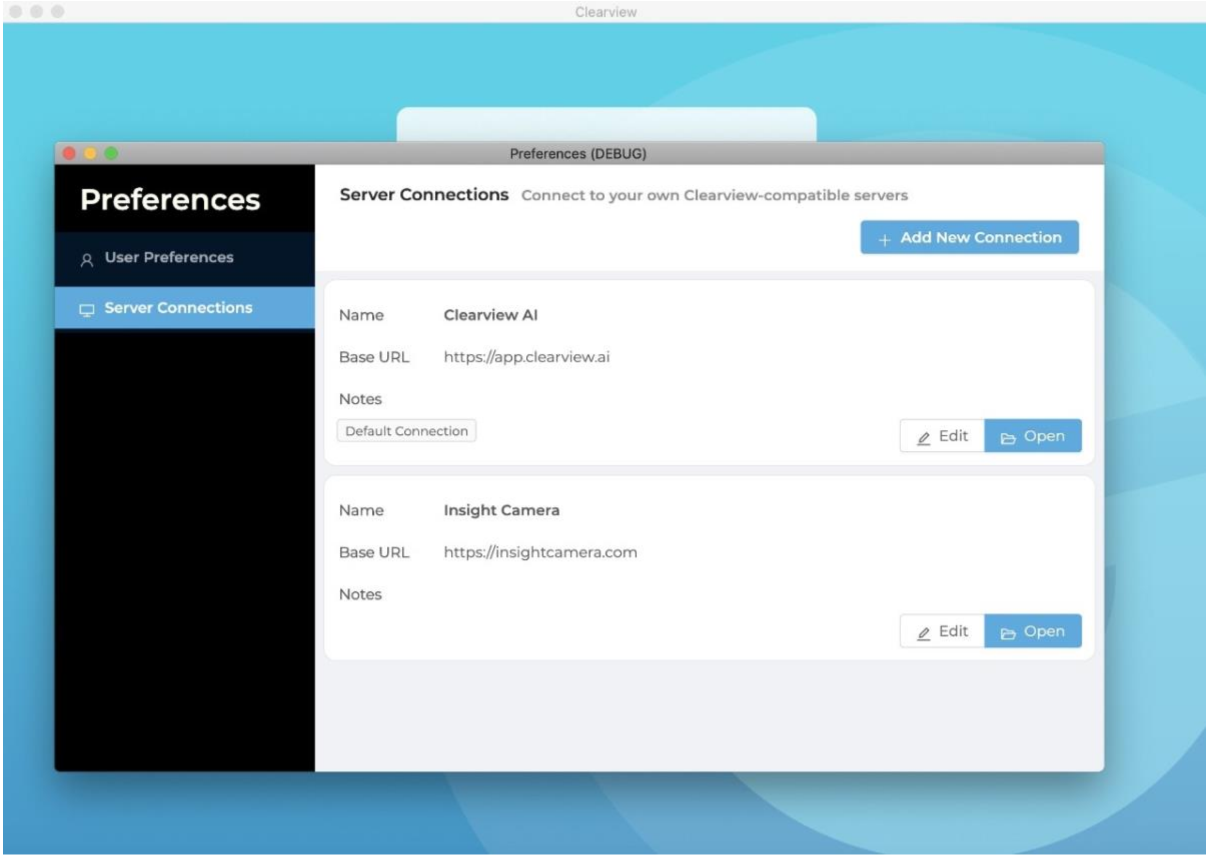
- When the start-up was reached for the comments on the security lapse, the Clearview AI's founder said they have set up a bug bounty program with HackerOne for finding the flaws in their systems. He also added that SpiderSilk was not a part of their bug bounty program and found a flaw in the Clearview AI and reached out to them, but did not expose any Personally Identifiable Information (PII), search history, or biometric identifiers.



(Whittaker 2020)

- Clearview Ai's IOS app did not need a log-in, and also Hussein took screenshots of how the app works. He used Mark Zuckerberg's photo as an example.

- Ton-That said that they had done a full forensic audit of the host to confirm that there is no other unauthorized access that has occurred, and also they have changed the secret keys in the storage buckets.



Server Connections Connect to your own Clearview-compatible servers

Name Clearview AI

Base URL https://app.clearview.ai

Notes

Default Connection

Name Insight Camera

Base URL https://insightcamera.com

Notes

(Whittaker 2020)

- The security officer also shared a screenshot of the code, and the apps referencing the company's insight camera. It was described as a prototype camera, and it was discontinued after this screenshot was made public.

- There were about 70,000 videos taken from a camera installed at the face-height in the lobby of a residential building, and this was also stored in a cloud storage bucket of Clearview Ai.

- Ton-That explained that it was a part of the prototyping security camera, and the videos were collected for debugging purposes with the permission of the building management.
- In defence of his company, the founder said that if the information is public and inside Google's Search engine, it can be inside Clearview AI as well. (Whittaker 2020)

II. Transparency and Explainability

- The New Jersey cops were told to halt the use of facial recognition technology by their state attorney general. Initially Clearview's promotional video featured attorney general Grewal and two state troopers at an October press conference about an operation, in which 19 men were arrested in New Jersey who tried to lure children for sex. Clearview takes partial credit in those recent arrests.

- But Grewal said it was irresponsible to reveal the investigation techniques and sent a cease-and-desist letter to stop using the footage in their promotional video. The footage was taken down from the company's website.

- Grewal had asked the county prosecutors to figure out what agencies are using Clearview as the company did not respond to the questions about how they are protecting the data or how many agencies have tried it. He also said that the department will not be using the technology until they respond to all the questions.

- According to Sarah Fajardo policy director for the ACLU in New Jersey, the tool can be used for constant and warrantless searches because of the lack of regulation. (Nelson 2020)

III. Accountability and responsibility

- Australian police agencies denied using the Clearview AI service initially. But the company's list of customers was breached, which revealed the users from the Australian Federal Police and the state police of Queensland, Victoria, and South Australia.

- It might have been the situation that the management at the law enforcement agencies were not aware that their employees were using the Clearview AI software.

The free trials of the software are given to the "active law enforcement personnel," but the verification procedure for using the software is not clear apart from owing a government email address.

- To be held accountable, the technology used by law enforcement should have been tested by the standard body to assure that it is fit. Clearview AI developers claim their software is 100% accurate, but the report is not generated by any standard body in US like National Institute for Standards and Technology. Instead the report was given by three people, chosen by Clearview AI and the reasons are unknown.

- A test was conducted by ACLU, where the images of 28 politicians were used against a mugshot database and as there were no matches, the system was said to have a good accuracy. The images of politicians were used for testing which is not a realistic scenario as the law enforcement agencies have to work with the poor-quality images from the surveillance or the CCTV cameras. There is no clear understanding about the how the software will work for the law enforcement and who will be held responsible for a false identification (Goldenfein 2020).

IV. Social impact and human well-being

- The head of Data protection at law practice JMW Solicitors, Toni Vitale, said that to conduct data scraping, six lawful bases are available under GDPR that Clearview should abide. The potential fitting lawful ground is a legitimate interest.
- Legitimate interest allows the scraping of data, if it is necessary for the business. Except that these interests should not override the fundamental rights and the freedom of individuals.
- Even if a company can establish a lawful basis, not all personal data can be scraped, although some social media sites allow scraping with their written prior permission. Explicit consent is needed to scrape data such as race, religion, political opinions, health data, so on. (Scroxton 2020)

Best possible practices or Legal Codes of Practice That could deal with the above discussed concerns

1) Clearview has violated multiple privacy laws, according to Mutnick, the representative of the **Chicago** civil rights firm Loevy & Loevy. He was the first one to file a lawsuit against Clearview, and he is seeking to get a court order to stop the company from selling the data. Attorney Jay Edelson also filled a case intending to obtain a court order for shuttering the company (Davis 2020).

2)

   a) The **American Civil Liberties Union** has sued Clearview AI for the violation of Illinois **BIPA** (Biometric Information Privacy Act) as the company has collected and stored the data without consent and has also sold the data to law enforcement agencies and private companies. BIPA is the only part of the US legislation that protects the biometric facial recognition data from misuse (Statt 2020).

b) Clearview announced that it would not be selling the technology to private companies. The company said that it would not be collecting the data from the IP address based on Illinois, and prevent the data collected from the Illinois residents with the help of an opt-out tool. But there is no clear picture of what steps are being taken to do it.

c) Clearview is continuing to store the information on the Illinois citizens. It is still subject to BIPA and hence allowing **ACLU** to team up with the local Illinois chapter and file another lawsuit. The demand is to ask Clearview AI to delete all the data it has collected and stop collecting the new data until it can comply with BIPA's consent rules (Alba 2020).

3) In January 2020, another lawsuit was filed against the Clearview app by the citizen of Illinois and called it an insidious encroachment on civil liberties and claimed that the company acted out of pure greed (Reichert 2020).

4)

a) The citizen of California registered a complaint. It does not plead a claim under the **CCPA** (California Consumer Privacy Act) itself, but it defines a "CCPA class" of California individuals whose data is being used by Clearview without prior notice and consent. The complaint then claims as follows under California's Unfair Competition Law, Business & Professions Code § 17200 (UCL), citing violations of the CCPA as underlying "unlawful" activity. Specifically, the complaint alleges as basis of UCL claim that the company collected the personal information as defined in the CCPA and failed to inform before or during the collection of data.

b) But it's unclear that the CCPA is employed in such a fashion, i.e., because of the "unlawful" activity supporting a UCL claim. The CCPA includes a particular provision, section 1798.150(c), that appears to ban precisely that variety of use: (c) The reason behind action established by this section shall apply only to violations as defined in subdivision (a) and shall not be supported violations of the other section of this title. Nothing during this title shall be interpreted to function the premise for a non-public right of action under the other law (Shreve & Sosnicki 2020).

5) The attorney general of Vermont TJ Donovan said that the company's business practices are disturbing as it includes the collecting and selling of children's facial recognition data. He also said that the database violates the **Vermont Consumer Protection Act and the Data Broker Law**.

6) Apart from these laws, the tech giants YouTube, Facebook, LinkedIn, and Twitter asked Clearview to stop scraping the images from their sites as they have their terms of service that forbid the scraping the information (Porter 2020).

Existing and potential technologies to deal with the discussed concerns.

1)

a) Facial recognition has to be implemented ethically and by protecting privacy. A safer approach and an effectively regulated way of using facial regulation models are to recognize similar faces and maintain a small watchlist of only the relevant names and faces by each of the individual law enforcement agencies. This approach will limit the amount of data lost in a potential data breach, but it will also give an oversight about how the data is being collected and used.

b) An attorney and visiting scholar at the Boston University School of Law, Tiffany C. Li, says that at this point where facial recognition technology is already out there in the world. There are various Implementations in the public and private sectors. Even if Clearview software is not used now, someone will use this technology to make a copycat software.

c) One of the best options is to regulate both the creation and the use of this technology. It is easy to say that companies like Clearview AI should be regulated, but it's more complicated when it is viewed as a bigger picture. In addition to the laws by which the companies building these technologies should abide, there should be a built-in recourse for individuals to protect their privacy and their rights (Ng 2020).

2)

a) The privacy scholar Frank Pasquale says that our current way of dealing with privacy is broke, and we can't expect individuals to keep track of all their gathered data and what is done with that data.

b) According to him, a temporary ban on the use of this technology would give the regulators a chance to catch up with advances in technology, which happens at the speed of light. The dangers of Facial recognition, including the tendency to misidentify the individuals and foster bias, are required for the organizations to have approvals in place before operating with the data. Private entities should obtain a license from the government authorities by specifying the nature of the approved use, specifying modes of recourse for that adversity impacted, and vetting the validity of the underlying data.

c) In the case of Clearview AI, it is going to be a tough situation as the technology is already out in the world (Pringle 2020).

3)

a) A unique footprint has to be identified, as not all data protection risks are created equal. The focus should be on the type of data that should be collected, processed, and stored. Privacy tools like data mapping and the privacy impact assessments are some excellent starting points to identify the company's unique footprint.

b) After this, the right-size of the risk profile should be found. Overestimating the risks hinder the growth and underestimating the risks can derail the business. Technical and legal are the ways to bring clarity about the uncertain risk scenarios. By doing these, it is helpful to identify the controls correlated with reducing data protection risks and, consequently, the liability exposure of the organization.

c) The results of data mapping and PIAs should be shared with the stakeholders, such as security and legal teams. Security teams can make use of the results to identify the additional controls necessary to safeguard processes that touch-sensitive data. The controls should include a strict code review for the modules that allow the data to share with third parties for a legitimate purpose. Unit tests should be included to ensure the ability to share the data, such as using an application programming interface endpoint, which is enabled or disabled only for a specified purpose.

d) Legal teams can use the input to ensure compatibility between the business objectives and data protection obligations and to put the necessary legal protections in place in the contracts. The protections should include an opt-in requirement to authorize the sharing or use of consumer data for a commercial purpose not covered as a legitimate business concern.

e) An operational cybersecurity program acts as a defence in case of accidental breaches. Businesses often view compliance as a burden and question the value it brings to put effort into a compliance framework.

f) But governance activities such as documentation of security procedures and practices, as well as certification of adherence to an established security standard, which is helpful to demonstrate the reasonableness of the security program that can help to mitigate legal consequences for the business (Bhatti 2020).

Conclusion

When a company like Clearview fails to keep the data secure, this might destroy the rights to anonymity and privacy (Alba 2020). If a password or a credit card number is breached, it can be changed or cancelled, but if the biometric data like facial characteristics are breached, it is not possible to change the faces. Hence it could be harmful to the individuals who want to hide their identities from people who seek to harm them.

The entire business model of Clearview AI relies on collecting sensitive and personal information, and the breach of such data is a sign that the potential benefits of the company's technology do not outweigh the grace privacy risks that it poses (Snider 2020). Every new technology has perspectives and promises for the future. There are several pros of biometric facial recognition technology, including criminal identification, healthcare, and others. It is quite clear that there is a line of difference between national security and invading people’s privacy that should not be crossed, which the progress in the technology.

Bibliography

- Clearview AI 2020, *Technology to help solve the hardest crimes*, Clearview AI, viewed 2 April 2020, < https://clearview.ai/>
- Cimpanu, C 2020, ‘Class-action lawsuit filed against controversial Clearview AI startup’, Zero Day, 24 January 2020, viewed 2 April 2020, <https://www.zdnet.com/article/class-action-lawsuit-filed-against-controversial-clearview-ai-startup/>
- Goldenfein, J 2020, ‘Australian police are using the Clearview AI facial recognition system with no accountability’, The Conversation Media Group Ltd, 4 March 2020, viewed 2 April 2020, <https://theconversation.com/australian-police-are- using-the-clearview-ai-facial-recognition-system-with-no-accountability-132667>
- Wikipedia 2020, *Clearview AI*, viewed 2 April 2020, <https://en.wikipedia.org/wiki/Clearview_AI>
- Whittaker, Z 2020, ‘Security lapse exposed Clearview AI source code’ *TechCrunch,* blog post, 17 April, viewed 20 May 2020, <https://techcrunch.com/2020/04/16/clearview-source-code-lapse/>
- Nelson,B 2020, ‘New Jersey cops told to halt all use of controversial facial-recognition technology’, *nj*, blog post, 24 Jan, viewed 21 May 2020, <https://www.nj.com/news/2020/01/new-jersey-cops-told-to-halt-all-use-of-controversial-facial-recognition-technology.html>
- Scroxton, A 2020, ‘Clearview hack fuels debate over facial recognition’, *Computer Weekly*, blog post, 27 Feb, viewed 20 May 2020, <https://www.computerweekly.com/news/252479248/Clearview-hack-fuels-debate-over-facial-recognition>
- Ng, A 2020, ‘Clearview AI says the First Amendment lets it scrape the internet. Lawyers disagree’, *c|net*, blog post, 6 Feb, viewed 20 May 2020, < https://www.cnet.com/news/clearview-says-first-amendment-lets-it-scrape-the-internet-lawyers-disagree/>
- Reichert, C 2020, ‘Clearview AI facial recognition company faces another lawsuit’ *c|net*, blog post, 13 Feb, viewed 20 May, <https://www.cnet.com/news/clearview-ai-facial-recognition-company-faces-another-lawsuit/>
- Statt, N 2020, ‘ACLU sues facial recognition firm Clearview AI, calling it a ‘nightmare scenario’ for privacy’ , *The Verge*, blog post, 28 May, viewed 29 May 2020, <https://www.theverge.com/2020/5/28/21273388/aclu-clearview-ai-lawsuit-facial-recognition-database-illinois-biometric-laws>
- Shreve, J & Sosnicki, L 2020, ‘Clearview AI class-action may further test CCPA’s private right of action’, *JDSUPRA*, blog post,12 March, viewed 20 May, <https://www.jdsupra.com/legalnews/clearview-ai-class-action-may-further-14597/
- Davis, W 2020, ‘Clearview AI Hit With Biometric Privacy Lawsuit’, *PolicyBlog,* blog post,23 January,viewed 20 May,<https://www.mediapost.com/publications/article/346121/clearview-ai-hit-with-biometric-privacy-lawsuit.html>
- Porter, J 2020, ‘Vermont attorney general is suing Clearview AI over its controversial facial recognition app’, *The Verge*, blog post, 11 May, viewed 20 May 2020, <https://www.theverge.com/2020/3/11/21174613/clearview-ai-sued-vermont-attorney-general-facial-recognition-app-database>
- Pringle, R 2020, ‘Controversial Clearview AI app could 'end privacy.' So, what now?’, *CBC*, 1 Feb, viewed 20 May 2020,<https://www.cbc.ca/news/technology/clearview-app-privacy-1.5447420>
- Bhatti, R 2020,‘Breaches at our front door: What we can learn from Clearview AI’, *IAPP*, blog post, 19 March, viewed 20 May 2020, <https://iapp.org/news/a/breaches-at-our-front-door-what-we-can-learn-from-clearview-ai/>
- Alba, D 2020, ‘A.C.L.U. Accuses Clearview AI of Privacy ‘Nightmare Scenario’’, *The New York Times*, 28 May, viewed 30 May 2020, <https://www.nytimes.com/2020/05/28/technology/clearview-ai-privacy-lawsuit.html>

- Snider, M 2020, ‘Clearview AI, which has facial recognition database of 3 billion images, faces data theft’, *USA Today ,* 27 Feb, viewed 20 May, <https://www.usatoday.com/story/tech/2020/02/26/clearview-ai-data-theft-stokes-privacy-concerns-facial-recognition/4883352002/>

Appendix:

The word count of the document is: **2719** words