TOR EKELAND LAW PLLC

Tor Ekeland
Partner
(718) 737-7264
tor@torekeland.com

June 12, 2020

Hon. Eddie Bernice Johnson
Chairwoman

Hon. Frank D. Lucas
Ranking Member

Hon. Bill Foster
Subcommittee Chairman

John Piazza, Esq.
Chief Counsel

Committee on Science, Space, and Technology
United States House of Representatives
2321 Rayburn House Office Building
Washington, DC 20515
(202) 225-6375

Re: Clearview AI

Chairwoman Johnson, Ranking Member Lucas, Chairmen Foster, & Mr. Piazza:

I write in response to your May 26, 2020 letter. Clearview AI shares your commitment to accuracy, reliability, and responsibility. Clearview's mission is to help public safety. Arresting the wrong people because of false identification hurts that mission because it deprives an innocent person of their liberty while leaving the guilty free to cause more harm. Fortunately, Clearview is part of the latest generation of facial recognition technologies that don't suffer from the bias of early versions.[1] And, to date, Clearview AI is unaware of any false identifications resulting in an arrest or conviction for anyone; its critics only allege speculative harms based on a misunderstanding of how Clearview AI's public photo search engine works. This misunderstanding has potentially dangerous consequences for the free flow of information on the internet.

Before the government can regulate the public's use and access to public information, it must obey the First Amendment. To date, no one has advanced a coherent legal explanation as to

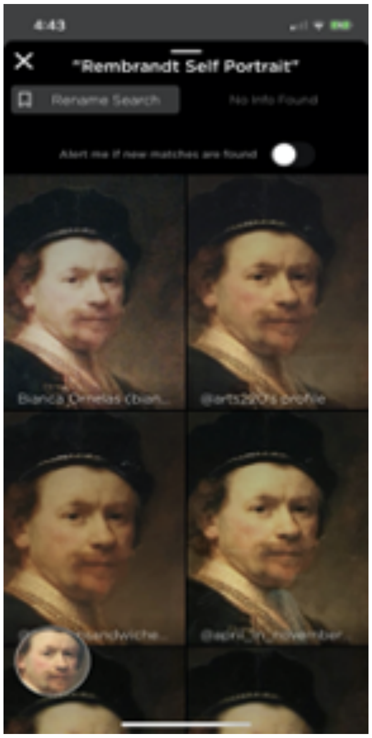
[1] *See About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies, Part II: Hearing before the H. Comm. on Homeland Security*, 116th Cong. 6 (2020) (Testimony of John P. Wagner) (https://docs.house.gov/meetings/HM/HM00/20200206/110460/HHRG-116-HM00-Wstate-WagnerJ-20200206.pdf) (last accessed June 12, 2020).

what gives the government the right to regulate public search engines and their expressive speech. Government regulation of search engines is no different than the government telling people what books they can check out and read from the library; or what pictures they can look at in an art museum.

Clearview AI's search engine is an internet search engine like Google or Bing. Clearview uses bots that crawl the internet indexing, copying, and caching publicly available information. Like Google, Bing, and many companies, Clearview AI caches the images it collects on servers to make searches more efficient. The servers caching this publicly available data are the same used by major financial institutions and Fortune 500 companies. Search engine technology would slow to a snail's pace without copying and caching information in this manner. Search engine speed comes from indexed information on a quickly available server. All the data Clearview collects is publicly available to anyone with an internet connection; Clearview's dataset is like Google's except that Clearview collects far less information than Google or many companies operating on the internet. And it doesn't use information to profile, track, or sell to people. That's for other search engines and smartphone Apps to do.

Clearview AI doesn't collect what federal law calls Personally Identifying Information ("PII"). The Office of Management and Budget Memorandum the Committee cites for its definition of PII isn't federal law. Regardless, Clearview doesn't intentionally collect names, addresses, social security numbers, account numbers, or the like. Nor does the App match names to photos. All the App collects are public photos from public servers, and whatever incidental metadata may be attached to that photo if any. Clearview uses neural net technology to render a photo into a readily searchable numerical hash, which represents that photo. These hashes are stored on secured servers separate from the photo database. Only approximately 10% of all pictures indexed by Clearview contain EXIF metadata which identifies the geolocation of where the photo was taken.

The image to the right is an image of a search run via the App on an iPhone of Rembrandt's Self Portrait at the Norton Simon Museum in Pasadena, California. The small circle with the face of Rembrandt on the bottom of the page is the original photo of the Rembrandt at the museum, the other photos, 325 that you can scroll through, are matches with pictures on the internet. If you tap any of the photos you are linked to the public website where that photo is located. That is the extent of what a user sees when they use the App. Note that nowhere are the photos identified as Rembrandt, and the names that do appear on the images are the public URL's to the sites that have the photo. It's the investigator who determines the identity of the photo search results by following the public links. And unlike forensic results with DNA or Fingerprints, facial matches between two photos are easily checked for accuracy with the naked eye. And indeed, that is what police whose departments use Clearview are trained to do by their internal training staff.



As a criminal defense lawyer, I share your concern over the potential for law enforcement abuse. A court sentenced one of my clients to three and a half years in federal prison because of a poorly written law known as the Computer Fraud and Abuse Act, justly known as "the worst law in technology." Part of that unjust prosecution involved an expansive interpretation of PII that included email addresses. For the nonviolent offense of accessing public information on the public internet from a publicly facing server, he spent over a year in prison before we got his conviction reversed. A large part of that year he spent in solitary confinement, which the United Nations, and I, consider to be torture. All because he copied a list of email addresses and sent them to the press.

The caching and use of publicly available photos and a face-matching algorithm isn't the threat. Facial identification is like any other powerful tool: neutral but capable of being used for good or evil. During the recent protests, there were numerous calls to identify police officers based on their photos. In at least one instance, facial recognition was used to identify and arrest someone who assaulted protestors.[2] And if this was done through public access to, and use of, public data it's protected by the First Amendment.

According to Canadian media, the FBI has tripled its ability to identify child predators and child sexual abuse victims online using Clearview's technology.[3] The innocent victims of crime—whether it be child sexual abuse and revenge porn online, fentanyl trafficking, or gun violence—rely on law enforcement to identify and prosecute those who harm them. Clearview's search engine is a crucial tool for vindicating victims with proven results. To date, no one has identified a single concrete, actual harm caused by Clearview.

Clearview's technology is neutral, and the First Amendment protects Clearview just as it protects every other search engine. To single out Clearview for its search engine results or algorithms, while saying nothing about the pervasive, real-time surveillance of Americans conducted by companies like Google, Amazon, Facebook, and Bing is content-based and speaker-based discrimination that violates the First Amendment. Nor does Clearview turn over reams of personal tracking data like these companies routinely do to law enforcement. Because Clearview doesn't collect the personal data these companies harvest, analyze, and monetize. Clearview merely copies public photos and analyzes them for matches with an inputted photo. To claim a right to regulate public access to public data, and the use of that data, has broad implications for science, academia, art, and a wide range of human endeavors. If computer languages, and the expressions of mathematical algorithms embodied in search engine results are to be regulated there must be a justification that meets strict scrutiny under the First Amendment. Because forbidding the publication of expressive search engine results is censorship. The First Amendment forbids Congress or the States dictating how people can access and use public information on the internet.

[2] *See* Dan Morse and Dana Hedgpeth, "*Arrest Made in Case of Bicyclist Accused of Assaulting Teens Posting Fliers on a Montgomery Country Trail*," Wash. Post, June 5, 2020, available at https://www.washingtonpost.com/local/public-safety/police-have-a-strong-suspect-in-case-of-bicyclist-accused-of-assaulting-teens-posting-fliers-on-a-montgomery-county-trail-official-says/2020/06/05/1cc57c0c-a752-11ea-b619-3f9133bbb482_story.html.

[3] *See* https://twitter.com/bpcarney/status/1250692551176261637/photo/2.

TOR EKELAND LAW PLLC

Tor Ekeland
Partner
(718) 737-7264
tor@torekeland.com

Here's our answers to your questions (in bold) from your May 26, 2020 letter:

1. **Mr. Ekeland's March 17 response said that "*we don't match names, addresses, or other forms of personally identifying information with a photo.*" Is it Clearview AI's position that biometric data by itself, including facial images, are not a type of PII?**

Under federal law Clearview does not collect PII. The Office of Management and Budget Memorandum you cite is not law. And any law regulating biometric information is subject to strict scrutiny under the First Amendment because computer languages, including search engine algorithms and the results they publish, are expressive speech. To hold otherwise is to invite government censorship of the internet.

2. **Please describe the basic security protocols that Clearview AI uses to protect and anonymize the biometric information it stores on its servers, including cryptographic hashing or other anonymization or de-identification efforts, as well as to protect against unauthorized system access, such as bug bounties and internal security assessments.**

When a user inputs a photo for a search the user's photo is run through Clearview's proprietary neural net algorithm which uses 512-points on an image to create a numerical representation of the image, called a "vector" or "hash," matching up with the geometry of the face. The user photo's vector is then run against Clearview's database, which have already been vectorized, to identify other images that are very similar to the searched. The user photo is not indexed or copied into Clearview's photo database.

Clearview's database of photos is comprised solely of publicly available photos and is stored on secure, industry-grade servers used by major financial institutions, with controlled access by only a few authorized individuals.

The vectors/hashes that Clearview generates for each image collected are also stored on a secure server with controlled access to only a few authorized individuals. This information is stored separately from the database of photos. The vectors/hashes of faces cannot be used outside Clearview's platform.

Clearview operates a bug bounty program through HackerOne, the industry leader in bug bounty programs. Clearview also commissioned a vulnerability assessment from NCC Group, the industry leader in security assessment and consulting. All the vulnerabilities identified by this assessment are being addressed. Clearview has added additional user password strengthening and verification requirements to its App and has introduced two-factor authentication. Clearview has an ongoing commitment to cybersecurity and work for constant improvement.

3. **In our first letter, we asked if Clearview Al is currently in contract negotiations with any foreign governments to provide products and services. Please address this question.**

a. **In addition, please provide a <u>complete</u> list of all foreign government agencies <u>and</u> all foreign-owned businesses to which you have at any time provided products and services, on either a paid or unpaid basis.**

Clearview is happy to provide information regarding the types of clients they work with; however, their client list itself is confidential.

4. **Does Clearview Al follow any Department of State or Department of Commerce guidance on export of its services? Please elaborate**.

Clearview acts in accordance with all applicable laws and regulations.

5. **Mr. Ekeland's March 17 response notes that Clearview "*restrict[s] access to [its] image database to only a small number of employees with the highest administrative access.*"**

a. **How many employees constitute a small number?**

Three employees who are subject to confidentiality agreements.

b. **Does Clearview have internal policies to prevent these employees from searching Clearview' databases for personal use? If so, how are these policies enforced?**

Clearview does not allow employees to use its search tools for personal purposes, and employee search activity is subject to review to enforce this policy.

6. **Clearview has touted the contributions of its technology to law enforcement efforts to identify victims of child sexual abuse imagery.**

a. **Does Clearview store the images it indexes of child sexual abuse imagery on its own servers?**

Clearview does not index child sexual abuse imagery or any other explicit images. Law enforcement personnel can use cropped images of victims or perpetrators of child sexual abuse to run a search on the platform, which will return other images of that person, aiding identification. Clearview does not possess any child sexual abuse imagery. Clearview does not store any images which are searched against its database except as part of secure, private client search histories which can be regularly purged. Clearview does not index images which are explicit in nature.

b. **If so, does Clearview apply any enhanced cybersecurity controls for the protection of these sensitive databases?**

As indicated above there is no data to apply enhanced protection to.

c. **How does Clearview limit the access of the employees it has granted access to its image databases generally to images of child sexual abuse imagery? Are access protocols for Clearview employees the same for databases containing images of children the same as they are for images of adults?**

No explicit images of any kind are stored.

7. **Mr. Ekeland's March 17 response to the Committee suggests that Clearview Al access is only granted to organizations "*with a legitimate need for [Clearview's] technology*." Clearview also published a blog post on January 27, 2020 suggesting that the technology is "*available only for law enforcement agencies and select security professionals to use as an investigative tool...and for legitimate law enforcement and security purpose only*." How do you define a "legitimate need" for Clearview's technology?**

Clearview's search platform is currently only available to federal, state or local law enforcement agencies. We define "legitimate law enforcement and security purposes" to mean protecting the public safety which includes investigating criminal activity and threats to national security as well as minimizing the risk of wrongful convictions based on false identification. It is to be used solely as an investigative tool.

8. **Public reporting suggests that company investors, and potential investors, have been granted wide access to Clearview's technology for their personal (non-investigative) use?**

a. **Can you confirm whether any company investors and potential investors retain the active access to Clearview's technology for their personal use?**

Investors do not currently have access to any Clearview technology. Potential investors are allowed temporary, limited access and may run searches on themselves or on other individuals who have provided consent, merely to perform their due diligence by witnessing the functionality of the technology.

b. **Does Clearview continue to offer the ability to conduct searches of its databases to potential investors or others without a paid subscription?**

As noted above, potential investors have limited, temporary accesses to test Clearview’s technology for due diligence purposes. The only other persons who retain access are law enforcement personnel and Clearview employees.

9. **Clearview’s January 27 blog post suggests that the company suspends or terminates users who violate its Code of Conduct.**

a. **How does Clearview determine when a use has violated the Code of Conduct?**

The determination of when a violation of the Code of Conduct has occurred is made by a review of the alleged violation by legal counsel.

b. **How many users has Clearview suspended for violating the Code of Conduct?**

Clearview takes enforcement of the Code of Conduct seriously and revokes user access as when reasonable suspicion of a violation arises. Information regarding specific users is confidential.

c. **Did Clearview investigate potential violations of the Code of Conduct following the March 5, 2020 New York Times article about non-law enforcement users of Clearview’s technology?**

Because all non-law enforcement users of Clearview’s technology have had their access revoked, including investors and potential investors, Clearview did not investigate any individual instances of use that may have violated their Code of Conduct.

d. **If so, did Clearview issue any suspensions or terminations as a result?**

As noted above, all non-law enforcement users have had their access to search technology terminated.

e. **Please provide a copy of Clearview’s Code of Conduct.**

Please see the attached Code of Conduct.

10. **Has Clearview Al participated in any accuracy benchmarking testing through the Department of Homeland Security's Biometric Technology Rallies or the National Institute of Standards and Technology's Facial Recognition Vendor Test program? Does Clearview Al intend to participate in such events to test the accuracy of its facial recognition algorithm across different demographics?**

In October of 2019, Clearview AI conducted an Accuracy Test Report. The test was undertaken in order to measure Clearview AI's performance in terms of accuracy across all demographic groups. For the purposes of this analysis, the Panel used the same basic methodology used by the American Civil Liberties Union (ACLU) in its July 2018 accuracy test of Amazon's "Rekognition" technology. Along with analyzing all 535 members of Congress, the Panel also analyzed all 119 members of the California State Legislature and 180 members of the Texas State Legislature, for good measure. The test compared the headshots from all three legislative bodies against Clearview AI's proprietary database (at that time) of 2.8 billion images (112,000 times the size of the database used by the ACLU). The Panel determined that Clearview AI rated 100% accurate, producing instant and accurate matches for every one of the 834 federal and state legislators in the test cohort. Accuracy was consistent across all racial and demographic groups within the dataset of legislators.

Clearview also tested the accuracy of their technology using the Megaface benchmark test—a 1 million photo dataset containing over 690,000 unique individuals which is made public for facial recognition algorithm evaluation by the University of Washington. The Megaface test is recognized worldwide as a leading method for evaluation of facial recognition accuracy. Algorithms are assessed by their ability to correctly match sample faces out of this dataset. Clearview conducted their Megaface test internally in late 2018, with an accuracy rate of 99.6% for the toughest Facescrub challenge. It measures the true positive rate of picking out a face accurately out of a gallery of 1 million other faces. Additionally, as indicated above, Clearview independently replicated and exceeded the ACLU's facial recognition evaluation test with 100% accuracy.

As for Clearview AI potentially participating in future testing of its technology, including through the Department of Homeland Security's Biometric Technology Rallies or the National Institute of Standards and Technology's Facial Recognition Vendor Test program, Clearview has not undergone the NIST to date due to the expense and logistics involved. Clearview's code is incompatible with NIST in its present form and as such would require a complete translation of code into a new programing language for the test to be carried out.

Please don't hesitate to contact me should you have any further questions. We welcome the opportunity to work with the Committee to craft constitutional standards for the use of this important technology.

Sincerely,

Tor Ekeland

cc: Hoan Ton-That; Richard Schwartz; Jack Mulcaire

EXHIBIT A

Clearview AI - Code of Conduct

Clearview AI, Inc. makes its software tools available to law enforcement and security professionals who will use them to enhance public safety and reduce crime, fraud, and risk in order to make communities safer. As a company, we hold ourselves to the highest level of commitment to ethics, integrity and professionalism. We take every step necessary to ensure that the search tools we provide are used correctly and lawfully. Our User Code of Conduct was developed to ensure that our customers are using Clearview in a safe, ethical, professional and appropriate manner. Users should review the Code carefully before activating their Clearview account in order to make certain they will be able to adhere to these essential rules of use.

This User Code of Conduct applies to all individual users (persons who possess an individual login associated with a particular email address and password to an account on the Clearview app, hereafter, “user”, “users”,or “individual users”) and to all user organizations (organizations which have concluded a Service Agreement with Clearview AI, hereafter “user organization”, “user organizations”, or “organization”).

By registering a user account with Clearview, and by using the web application and the Clearview mobile application (collectively, the “Clearview app”), individual users and user organizations agree to be bound by this User Code of Conduct (this “Code”).

Account Security

Users are responsible for maintaining the confidentiality of their username and password.

Users are responsible for all activities that occur under that user’s username and password. Users must immediately email the Clearview Help Desk at help@clearview.ai to notify Clearview AI, Inc. of any unauthorized use of their username or password or any other breach of security.

Users may only access their accounts from devices that are authorized for professional use by their user organization.

The designated user is the only individual who may access and use the account.

Independent Verification

Search results established through the Clearview app and its related systems and technologies are indicative and not definitive. Clearview AI, Inc. takes every step to ensure the accuracy of its facial recognition software.

However, it is not possible to guarantee the accuracy of the search results it produces. Users must conduct further research and investigation in order to verify the accuracy of any search result.

The Clearview app is neither designed nor intended to be used as a single-source system for establishing the identity of an individual, and users may not use it as such.

Furthermore, search results produced by the Clearview app are not intended nor permitted to be used as admissible evidence in a court of law or any court filing.

Appropriate and Authorized Use

The Clearview app may only be used by law enforcement and security professionals.

Users may only use the Clearview app for legitimate law enforcement and security purposes. All use of the Clearview app must be authorized by a supervisor employed by the user's organization.

User organizations must designate an Executive User ("Administrator"), who shall have access to the search histories of all individual users associated with the User organization, and shall monitor said search history to ensure responsible use.

Users may not use the Clearview app for personal purposes, or for any purposes which are not authorized and directed by the user organization's supervisors.

Use of the Clearview app in a fashion which contributes to harassment, stalking, cyberstalking, threats, abuse or bullying, or in violation of any state, federal or local laws, is strictly prohibited by this code of conduct.

Clearview AI, Inc. retains the right to suspend or terminate user accounts if we determine that a user or user organization has violated this section of the Code of Conduct.

Conclusion

Clearview AI, Inc. aspires to make the world a better place by helping qualified professionals use public information to stop crime and fraud through its proprietary technology. The Clearview User Code of Conduct is a key part of ensuring that our relationships with our customers are based on integrity, responsibility and professionalism.

We thank you for adhering to the User Code of Conduct. By doing so, you are helping us achieve our collective goal of making communities safer while adhering to the highest standards of ethics and security.