TOR EKELAND LAW PLLC

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

March 24, 2020

Via Email and FedEx

Hon. Edward J. Markey
United States Senator
United States Senate
255 Dirksen Senate Office Building
Washington, D.C. 20510
(202) 224-2742
Bennett_butler@markey.senate.gov

RE: Clearview AI

Dear Senator Markey,

We appreciate your on-going interest in Clearview AI's service. Clearview AI works hard every day to improve our service as a partner to American law enforcement. We also work with policymakers, like yourself, concerned with facial recognition technology. We believe that the enhancements to public safety this technology offers can be secured without impeding constitutional rights. In this case, public safety and constitutional rights aren't antithetical, as Clearview AI doesn't search for private photos.

As you're aware, open access to the internet is a hallmark to today's internet. Clearview AI is simply a photo search engine that limits itself to publicly available photos accessible to anyone who has an internet connection. Its dataset is the public internet's dataset. What's innovative about Clearview AI's software is its efficiency at matching input photos with publicly available online photos. Its dataset is available to anyone, indeed, it's just an infinitesimal subset of the vaster set voracious data miners like Facebook, Twitter, Google, Bing and other surveillance advertising companies vacuum up in real time on their users. Unlike those companies, Clearview AI doesn't even match photos with names, only providing the public URL to a photo for an investigator to follow up on and confirm. Clearview AI doesn't record information about anyone's movements, internet browsing habits, financial history, purchases, or private communications. We merely index public photos from the public internet and make it quickly searchable.

We share your concern in preventing abuse of this critical law enforcement tool. To date, we are aware of none. Fortunately, all the harm is speculative. We further share your

concern with regards to privacy alongside the core First Amendment principle of public access to public information on the internet. That's why use of Clearview AI is intended for legitimate law enforcement purposes, and why we are constantly working to improve the safety of our service. As Clearview AI emerges from its startup phase, adding more employees and improving our technological infrastructure, we look forward to a productive dialogue with policy makers as to the responsible use of this important public safety tool.

Here's our answer to your questions (in bold) from your January 22, 2020 letter:

1. **Please provide a list of all law enforcement or intelligence agencies that (A) Clearview has marketed to or otherwise communicated with regarding acquisition of your technology, and (B) currently use the Clearview service.**

   We are happy to provide information regarding the types of clients we work with; however, our client list itself is confidential. Hundreds of federal, state and local law enforcement agencies nationwide use our technology, either on a paid basis or as unpaid trial users. We advertise our software via email and online ads on law enforcement websites and email lists like Crimedex, and by attending law enforcement trade shows.

2. **Does Clearview market to or sell your service to any entities besides law enforcement? If yes, please list. If not, will Clearview commit to not expanding its customer base to private companies or individuals?**

   Clearview AI has worked with a small number of financial institutions, large retailers and private security companies to provide our technology for anti-fraud and security purposes. At present our only private clients are financial institutions.

3. **Please provide the results of any internal accuracy or bias assessments that Clearview has performed on its technology. Please provide this information broken down and in combination for race, gender, ethnicity, and age.**

   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. The Independent Review Panel determined that Clearview

AI rated 100% accurate, producing instant and accurate matches for every photo image in the test. Accuracy was consistent across all racial and demographic groups within the dataset of legislators.

4. **Please describe in detail how Clearview tests for facial recognition accuracy, how often Clearview performs such tests, and whether these results have been independently verified**.

   Clearview AI tested the accuracy of our 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. We conducted our 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. The only major company ranking higher than Clearview AI is SenseTime with a 99.8% accuracy, the largest facial recognition provider in China. Additionally, as indicated above, we independently replicated and exceeded the ACLU's facial recognition evaluation test with 100% accuracy.

5. **Does Clearview provide information and training regarding the accuracy rates of your technology to your users? If yes, please detail this training and information sharing. If not, why not?**

   Clearview AI provides education on how to use our technology for users in a number of different ways. These include in-person demonstrations and briefings on how to use it, online videoconferencing demonstrating the use of the software, and providing educational materials on how to use Clearview AI accurately, including information on reasons why no matches or inaccurate matches may appear (such as very low-resolution probe images).

6. **Have any law enforcement agencies that used or are using Clearview's technology been investigated, sued, or otherwise reprimanded for engaging in unlawful or discriminatory policing practices? Does Clearview consider whether law enforcement agencies have a history of unlawful or discriminatory policing practices when deciding to whom it will market or sell its technology?**

   Many law enforcement agencies have used Clearview AI, some for more than a year. To date, there has not been a single reported abuse of its software, despite intense investigative reporting by the New York Times and Buzzfeed. While Clearview AI can point to concrete examples where it helped solve serious crimes, its opponents only speculate when they describe its imagined harms. As Clearview AI emerges from its startup phase, adding more employees and improving our technological infrastructure,

we look forward to a productive dialogue with policymakers as to the responsible use of this important public safety tool.

7. **Can Clearview's technology recognize whether the biometric information uploaded to its systems includes children under the age of 13? If yes, does Clearview have any protections in place to ensure the privacy of such children, and how does Clearview ensure that it complies with the Children's Online Privacy Protection Act?**

   Clearview AI only indexes and stores public photos and their public URL. We don't match names, addresses, or other forms of personally identifying information with a photo. We only match a face on an inputted photo with a face on the public internet. Clearview AI follows internal standards and guidelines. The public spaces from which Clearview AI indexes photos are COPPA compliant. Clearview AI does not waiver from that COPPA compliant public space. As stated above, Clearview AI does not index or store personal information, such as age. Additionally, Clearview AI's activities fall outside of the scope of COPPA. The statute defines an operator as, in relevant part, "any person who operates a website located on the Internet or an online service and who collects or maintains personal information **from or about the users of or visitors to such website** or online service." (emphasis added). 15 USC § 1602 (a)(2). Because Clearview AI only functions as a search engine, indexing images from other websites, not users of our website, it falls outside of the statutory definition of "operator." This distinction is necessary to enable search engines to function.

8. **Do Clearview employees have access to the images that your customers upload onto Clearview's servers? If yes, what safeguards does Clearview have in place to ensure that employees do not breech the privacy of photographed individuals?**

   We restrict access to our image database to only a small number of employees with the highest administrative access. It is our policy to not access any client search histories (if the client has not disabled search history) unless the client requests it, or unless necessary to enforce the Terms of Service.

9. **Will Clearview commit to providing individuals with an effective process to have images of their faces deleted from Clearview's database upon request?**

   Clearview AI has already put in place a process by which individuals may request to have their images removed.

10. **Will Clearview commit that it will never integrate its technology with augmented reality glasses? Will Clearview commit that it will never integrate its technology with any other tools that would allow users to capture images and run them against Clearview's database in real-time, unbeknownst to the photographed individuals? If not, why not?**

Clearview AI is committed to upholding individual rights while assisting law enforcement agencies in protecting the physical and property rights of individuals. To that end, where real-time technological devices can be legally used in furtherance of legitimate law enforcement or national security goals, Clearview AI will continue to innovate in that space.

11. Please describe in detail the cyber security practices and procedure Clearview employs to protect the data it uses and stores. Does Clearview encrypt the facial recognition data it uses? How frequently does Clearview conduct security tests?

We restrict access to our image database to only a small number of employees with the highest administrative access. It is our policy to not access any client search histories (if the client has not disabled search history) unless the client requests it, or unless necessary to enforce the Terms of Service. Employees access Clearview AI on dedicated work devices. We regularly conduct cybersecurity testing and are constantly working to enhance the security of our platform.

12. Has Clearview detected any security breaches or incidents since its inception? If so, please detail these episodes, relay what government entities were informed of the episode, and describe the steps Clearview took to fix all relevant security vulnerabilities.

Clearview AI has never suffered a data breach that resulted in the disclosure of any personally identifiable information. The only incident of unauthorized access to any information possessed by Clearview AI was the February 2020 incident referenced in your March 3 letter, which did not result in the release of any information pertaining to law enforcement, beyond the list of client organizations, the number of accounts they hold and the number of searches they had performed.

13. Does Clearview conduct audits of its law enforcement customers to ensure that (A) the software is not being abused for secretive government surveillance, (B) the software is not facilitating systems that disproportionately impact people based on protected characteristics in potential violation of federal civil rights law, and (C) the software is not being used in violation of Clearview's terms of use? If so, what steps does Clearview take to end any such uses of its technology?

A small technology startup like Clearview AI cannot effectively act as a civil rights and internal affairs oversight body for American federal, state and local law enforcement. We request that user organizations assign an internal administrator, who can monitor the search histories of their Clearview AI users, to prevent misuse. When and if we become aware of our policies not being followed, we will suspend or terminate users as appropriate. We are also developing additional technological tools to further ensure appropriate use.

14. **Is Clearview's technology currently integrated with any police body-camera technology or existing public-facing camera networks? Please identify any government customers using Clearview's technology for continual, real-rime facial recognition of the public.**

    Clearview AI does not integrate our technology with police body cameras or public-facing camera networks.

Turning to your questions from your letter dated March 3, 2020:

1. **Does Clearview plan to sell its technology outside of the U.S.?**
    a. **If so, to whom? And if so, how can Clearview guarantee that its technology will not enable repression and human rights abuses?**

    We have permitted law enforcement organizations in foreign nations to engage in limited trial uses of our technology, including Canada, the United Kingdom, Australia, and New Zealand. Our only paid foreign client organization is the Royal Canadian Mounted Police. We believe that our product can be highly beneficial to the national security and public safety of America's global allies and are happy to provide it to responsible international partners, in a fashion consistent with the law both in the United States and in the relevant foreign nations.

2. **Please describe the steps Clearview has taken to ensure that it is in compliance with the Children's Online Privacy Protection Act.**
    a. **Does Clearview collect and process images of children under 13?**
        i. **If so, does Clearview provide notice or obtain parental consent? And in the absence of consent, what is the process for deleting such images?**
        ii. **If not, how does Clearview ensure that it does not collect or process pictures of children under 13 when scraping billions of pictures from social media?**
    b. **Does Clearview collect and process images and data from any platforms that are directed to children under 13 or allow children under 13 to be users?**
        i. **Please list the platforms from which Clearview scrapes data, the data that it scrapes from each of those platforms, whether that platform is directed to children under 13, and whether that platform allows children under 13 to be users.**
    c. **Does Clearview have reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children under 13? If so, please describe these procedures. If not, why not.**

    Clearview AI collects images from the open web and major social media platforms. As indicated above, the sites we index are themselves COPPA-compliant. Additionally, Clearview AI's activities fall outside of the scope of COPPA. The statute defines an operator as, in relevant part, "any person who operates a website located on the

Internet or an online service and who collects or maintains personal information **from or about the users of or visitors to such website** or online service." (emphasis added). 15 USC § 1602 (a)(2). Because Clearview AI only functions as a search engine, indexing images from other websites, not users of our website, it falls outside of the statutory definition of "operator." This distinction is necessary to enable search engines to function.

3. **Hackers recently breached Clearview's security and reportedly obtained your entire client list.**
    a. **Were any facial images or other personally identifiable information accessed as part of this hack? Please specify in detail what data was accessed.**
        i. **If personally identifiable information was compromised as a result of this data breach, will Clearview commit to notifying every individual whose data was compromised? If not, why not?**
    b. **What steps has Clearview taken, including changes to its security policies and technologies, to minimize the damage of this type of breach and to avoid future breaches of data?**
    c. **Has Clearview identified the individual or entity that perpetrated this security breach? If so, please provide that information.**

No facial images or any other biometric data was accessed as part of the cyber incident. Clearview AI has never suffered a loss of biometric data sense its inception. The information which was accessed in the February 2020 incident was limited to: our list of client organizations, the number of accounts they hold and the number of searches they had performed. The vulnerability that led to this incident of unauthorized access has been eliminated. We are enhancing our technological security measures as well. All users have been authenticated, all web routes have been audited for permissions issues, users are alerted when their accounts are logged into, a bug bounty program is being set up, IP logging has been added to the login history UI, and many additional improvements are in progress

4. **Clearview's website claims that its technology was "designed and independently verified to be in compliance with all federal, state, and local laws." Please describe the steps taken as part of this design and independent verification, and specify the federal, state, and local laws that were analyzed.**
    a. **In particular, please describe the steps Clearview has taken to ensure it is in compliance with Illinois' Biometric Information Privacy Act, which requires notice and consent in order to collect or store biometric information including pictures of faces.**

During 2019, we worked with former U.S. Solicitor General and former U.S. Attorney General Paul Clement and other lawyers at Kirkland & Ellis to assess Clearview's compliance with various laws, including the 4th Amendment and the Biometric

Information Privacy Act. It is our position that Clearview AI is covered by the government contractor exemption in the Biometric Information Privacy Act.

5. **Please identify the "select security professionals" and any other private entities or individuals that are current or former clients of Clearview.**

   As indicated above, Clearview AI currently provides our technology to security and anti-fraud staff at a handful of financial institutions. In the past, we have provided our technology to security employees at a small number of large national retailers and a handful of private security companies, but we have terminated those accounts out of an abundance of caution.

6. **What data or metadata does Clearview collect, in addition to the photos the company scrapes from social media?**

   Clearview AI is simply a photo search engine that limits itself to publicly available photos accessible to anyone who has an internet connection. The only metadata we collect is that which is attached to the photos. Clearview AI does not even match the photos to names, we only provide the public URL to a photo for an investigator to follow up on and confirm.

7. **Does Clearview have plans to integrate its technology and database with live facial recognition tools, such as augmented reality glasses? If so, will Clearview commit to halting all such integration given the grave privacy and civil liberty risks this would pose to the public?**

   Please see the answer to question number 10 above.

8. **Will Clearview commit to providing individuals with a way to delete their images from Clearview's database without having to provide their headshot and government ID?**

   As we do not collect any personally identifying information, aside from publicly available photos, it would be impossible for Clearview AI to provide individuals with a practical way of removing their images from our database without providing a headshot for Clearview AI's algorithms to use in the removal of their images. A government ID is necessary to ensure the individual requesting access or removal is the individual pictured, as Clearview AI can only identify a person based off of their image. The most widely available and acceptable form of identification of an individual's image and name is their government-issued photo ID and as such Clearview AI relies on these IDs to ensure legitimate requests can be honored.

9. **Many major internet companies have now sent your company cease-and desist letters for violating their terms of service by scraping their platforms for photos. Will**

Clearview comply with the cease-and-desist orders that it has received from internet platform companies such as Facebook, Google, and Twitter?

Our indexing activities are entirely legal—they do not violate the Computer Fraud and Abuse Act, copyright law, or any other type of law. Therefore, we believe the cease-and-desist letters we have received from various tech companies are legally baseless.

10. **Will Clearview commit to deleting any images that it has scraped from the aforementioned websites?**

    We will not delete the public photos we index from these public sites because - under both the First Amendment and federal case-law there is no legal obligation for us to do so. If individuals want to exercise their rights to data removal or copyright takedown under various laws, we provide processes to facilitate those types of removals.

11. **Will Clearview commit to deleting any AI or machine learning algorithms that it developed using images from the aforementioned websites?**

    Our facial recognition algorithm is legal, proprietary, and an innovative public safety tool.

12. **Will Clearview submit its technology for an independent assessment of accuracy and bias by facial recognition experts?**

    Clearview AI continues to improve the accuracy of our technology and we will continue to test and verify that accuracy. We have already dedicated significant resources to accuracy and bias testing by completing the Megaface test and by replicating and exceeding the ACLU's bias test. When appropriate, we will perform additional independent verification.

We appreciate your interest in our company and how we are using technology to help law enforcement to make communities and children safe. Please don't hesitate to contact me should you wish to discuss this further.

Sincerely,

Tor Ekeland

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