TOR EKELAND LAW PLLC

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

**March 17, 2020**

**Via Email and FedEx**

Hon. Eddie Bernice Johnson
Chairwoman

Hon. Frank D. Lucas
Ranking Member

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

Dear Chairwoman Johnson and Ranking Member Lucas:

Thank you for your letter. Clearview AI works hard every day to improve our service as a partner to American law enforcement. We also work with policy makers 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 doesn't search private photos.

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.

Thousands of 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 solved 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 policy makers as to the responsible use of this important public safety tool.

Here are our answers to your questions from your letter of March 3.

1. **Please provide a detailed description of how Clearview AI compiles the biometric data it uses in its facial recognition products. Please also describe where Clearview AI collects this data from and if any of this data is collected or purchased from third parties.**

Clearview AI uses proprietary technology, developed in-house, to collect images of persons from publicly accessible portions of the Internet. These images are then converted into hashes based on our proprietary facial geometry algorithm, also developed in-house. We collect data from the open web and from publicly accessible portions of social media platforms. Images that are behind privacy settings are not collected.

2. **Does Clearview AI follow any government or industry best practices or standards for the protection of personal data (i.e. privacy standards including any voluntary consensus standards? If so, please provide a comprehensive list of the standards. Does Clearview AI employ any third-party conformity assessments to ensure or measure compliance with any of these standards?**

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. Cybersecurity is a top priority for us, and third-party assessments are on our roadmap.

3. **Does Clearview AI limit access to its products and services? If so, how does Clearview AI determine who may access its products and services?**

Every application for an account with Clearview AI must be approved by a trained employee. The online submission requesting access is vetted to ensure that the relevant email address is attached to an existing domain of an organization with a legitimate need for our technology, and inquire using various methods from simple internet searches to phone calls to determine if the person in question is employed at that organization.

4. **Has Clearview AI ever allowed foreign owned businesses or foreign government agencies to access any of its products and services? If so, please provide a detailed accounting of the clients and services provided to non-U.S. clients, including any foreign governments. Is Clearview A.I. currently in contract negotiations with any foreign governments to provide products and services?**

We have permitted law enforcement organizations in foreign nations to engage in 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.

5. **Please describe in detail the cybersecurity practices and procedures that Clearview AI employs to protect both client data as well as the underlying data used in Clearview AI's facial recognition products. Specifically, does Clearview AI follow any cybersecurity standards issued by the National Institute of Standards and Technology? Does Clearview AI employ any third-party conformity assessments to ensure compliance with cybersecurity standards?**

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 on dedicated work devices. Currently we do not follow any third-party conformity assessments.

6. **How many data breach incidents have occurred at Clearview AI? Have any of these breaches resulted in the loss of biometric data of U.S. citizens? Have any of these breaches ever resulted in the release of law enforcement sensitive information?**

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 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.

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