EDDIE BERNICE JOHNSON, Texas
CHAIRWOMAN

FRANK D. LUCAS, Oklahoma
RANKING MEMBER

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6301

(202) 225–6375
www.science.house.gov

May 26, 2020

Mr. Hoan Ton-That
Chief Executive Officer
Clearview AI
214 W 29th St, 2nd Floor
New York, NY 10001

Dear Mr. Thon-That:

We wrote to you on March 3, 2020 raising questions about Clearview AI's approach to data privacy and cybersecurity matters.[1] We received a response on behalf of Clearview AI from your counsel, Mr. Tor Ekeland, on March 17. His responses, along with new information from recent public reporting, raise further questions for Clearview. In addition, Mr. Ekeland's answers did not adequately address some of the questions raised in the Committee's first letter.

Our concerns are compounded in light of recent reporting that the February 2020 hack of Clearview's systems exposed essentially all of Clearview's source code for its proprietary web scrapping tool to the public.[2] Despite Mr. Ekeland's claims that the February 2020 hack did not expose any personally identifying information (PII) or communications internal to the company, the exposure of source code would make it possible for anybody who tapped Clearview's repository to run their own searches and aggregate the biometric data of social media users. And as you may know, the Office of Management and Budget Memorandum M-07-1616 defines PII to include biometric data like facial imagery.[3]

At the very least, the possibility that Clearview's source code has been exposed to outside actors renders meaningless the assurances Clearview gave the Committee about its efforts to limit access to its platform to "*organizations with a legitimate need.*"

Please provide written answers to the following questions by June 9, 2020:

---

[1] https://science.house.gov/letter-to-clearview-ai-ceo-on-recent-data-breach.
[2] Whittaker, Zack. "Security lapse exposed Clearview AI source code." *TechCrunch.com.* April 16, 2020. Accessed at https://techcrunch.com/2020/04/16/clearview-source-code-lapse/.
[3] OMB Memorandum M-07-1616 defines PII as "info that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual."

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?

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.

3. In our first letter, we asked if Clearview AI is currently in contract negotiations with any foreign governments to provide products and services. Please address this question.
    a. In addition, please provide a complete list of all foreign government agencies and all foreign-owned businesses to which you have at any time provided products and services, on either a paid or unpaid basis.

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

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

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

7. Mr. Ekeland's March 17 response to the Committee suggests that Clearview AI 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 purposes only.*"[4] How do you define a "legitimate need" for Clearview's technology?

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.[5]

---

[4] https://blog.clearview.ai/post/2020-01-27-code-of-conduct/
[5] https://www.nytimes.com/2020/03/05/technology/clearview-investors.html

a. Can you confirm whether any company investors and potential investors retain the active access to Clearview's technology for their personal use?
b. Does Clearview continue to offer the ability to conduct searches of its databases to potential investors or others without a paid subscription?

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?
    b. How many users has Clearview suspended for violating the Code of Conduct?
    c. How many users has Clearview terminated for violating the Code of Conduct?
    d. 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?
    e. If so, did Clearview issue any suspensions or terminations as a result?
    f. Please provide a copy of Clearview's Code of Conduct.

10. Has Clearview AI 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 AI intend to participate in such events to test the accuracy of its facial recognition algorithm across different demographics?

Pursuant to Rule X of the House of Representatives, the Committee on Science, Space, and Technology has jurisdiction over the National Institute of Standards and Technology, which develops cybersecurity standards and guidelines for the federal government and recommendations for the private sector. Clearview AI's activities raise troubling questions about several issues in areas that the Committee oversees, including data privacy technology, artificial intelligence technology, cybersecurity technology, and the standards that may or may not accompany each of these technologies.

If you have any questions about this request, please feel free to contact John Piazza, Chief Counsel for the Committee, at 202-225-6375. Thank you for your attention to this matter.

Sincerely,

Eddie Bernice Johnson

Eddie Bernice Johnson
Chairwoman
Committee on Science, Space, and Technology

Bill Foster

Bill Foster
Chairman
Subcommittee on Investigations & Oversight
Committee on Science, Space, and Technology