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

March 3, 2020

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

Dear Mr. Ton-That:

We are deeply concerned about recent reports that indicated Clearview AI was breached and has "lost its entire client list to hackers."[1] One news source reported in detail that Clearview AI "disclosed to its customers that an intruder 'gained unauthorized access' to its list of customers, to the number of user accounts those customers had set up, and to the number of searches its customers have conducted."[2] Given that your company reportedly works extensively with law enforcement, we write to express our concerns about this data breach.

The reports about the recent data breach follow other reports about the work that your company is doing on facial recognition technology. The New York Times recently reported that Clearview AI has "scraped" billions of images from social media and similar websites to use in its application, and that the company has already worked with hundreds of law enforcement agencies, as well as some private companies.[3]

Clearview AI's work appears subject to very little government oversight, despite the serious privacy questions raised by the intended use of Clearview AI's technology. These concerns are compounded immensely by the knowledge that the firm has now been the subject of a successful hacking operation. We believe that Clearview AI needs to provide answers to some basic questions about how the company collects, uses, and protects U.S. citizens' data. Since we know that numerous law enforcement agencies already use your

---

[1] Jordan Valinsky, *Clearview AI has billions of our photos. Its entire client list was just stolen*, CNN (Feb. 26, 2020), https://www.cnn.com/2020/02/26/tech/clearview-ai-hack/index.html.
[2] Betsy Swan, *Facial-Recognition Company That Works With Law Enforcement Says Entire Client List Was Stolen*, DAILY BEAST (Feb. 26, 2020), https://www.thedailybeast.com/clearview-ai-facial-recognition-company-that-works-with-law-enforcement-says-entire-client-list-was-stolen.
[3] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Feb. 10, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

services, we also have questions about how data breaches at your company could affect ongoing law enforcement operations.

Please provide written answers to the following questions by Tuesday March 17:

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.
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?
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?
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 the services provided to those non-U.S. clients, including any foreign governments. Is Clearview AI currently in contract negotiations with any foreign governments to provide products and services?
5. Please describe in detail the cybersecurity practices and procedures 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?
6. How many data breach instances 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?

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
Chairwoman
Committee on Science, Space &
Technology

Frank D. Lucas
Ranking Member
Committee on Science, Space &
Technology