

EDWARD J. MARKEY
MASSACHUSETTS

COMMITTEES:

ENVIRONMENT AND PUBLIC WORKS

FOREIGN RELATIONS

RANKING MEMBER:

SUBCOMMITTEE ON EAST ASIA, THE PACIFIC,
AND INTERNATIONAL CYBERSECURITY POLICY

COMMERCE, SCIENCE, AND TRANSPORTATION

RANKING MEMBER:

SUBCOMMITTEE ON SECURITY

SMALL BUSINESS AND ENTREPRENEURSHIP

CHAIRMAN:

U.S. SENATE CLIMATE CHANGE TASK FORCE

United States Senate

SUITE SD-255
DIRKSEN BUILDING
WASHINGTON, DC 20510-2107
202-224-2742

975 JFK FEDERAL BUILDING
15 NEW SUDBURY STREET
BOSTON, MA 02203
617-565-8519

222 MILLIKEN BOULEVARD, SUITE 312
FALL RIVER, MA 02721
508-677-0523

1550 MAIN STREET, 4TH FLOOR
SPRINGFIELD, MA 01103
413-785-4610

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

Dear Mr. Ton-That,

I write regarding disturbing reports that your company, Clearview, is selling a facial recognition tool that could eliminate public anonymity in the United States. Any technology with the ability to collect and analyze individuals' biometric information has alarming potential to impinge on the public's civil liberties and privacy. Clearview's product appears to pose particularly chilling privacy risks, and I am deeply concerned that it is capable of fundamentally dismantling Americans' expectation that they can move, assemble, or simply appear in public without being identified.

A recent investigation published in the *New York Times* reveals that your product allows users to capture and upload photos of strangers, analyze the photographed individuals' biometric information, and provide users with existing images and personal information of the photographed individuals online.¹ The ways in which this technology could be weaponized are vast and disturbing. Using Clearview's technology, a criminal could easily find out where someone walking down the street lives or works. A foreign adversary could quickly gather information about targeted individuals for blackmail purposes. Widespread use of your technology could facilitate dangerous behavior and could effectively destroy individuals' ability to go about their daily lives anonymously.

I am also troubled to learn about reports that Clearview is actively marketing this technology to law enforcement departments across the country. Public safety professionals should, of course, employ new tools and techniques to keep our communities safe. However, use of new innovations to protect the public should not come at the expense of our basic privacy rights.

¹ Kashmir Hill, *The Secretive Company That Might End Privacy As We Know It*, *New York Times* (January 18, 2020) <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>.

Currently, the public lacks important information regarding the nature of Clearview's partnerships with law enforcement entities.

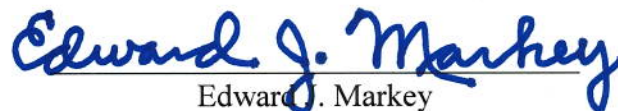
I request written answers to the following questions by February 12, 2020:

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

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?
11. Please describe in detail the cyber security practices and procedures 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?
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 episodes, and describe the steps Clearview took to fix all relevant security vulnerabilities.
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 laws, 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?
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-time facial recognition of the public.

Thank you for your attention to these requests.

Sincerely,



Edward J. Markey
United States Senator