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

March 3, 2020

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 wrote to you on January 23, 2020 with serious concerns regarding how Clearview's facial recognition product might intrude on Americans' civil liberties and privacy. Your January 31, 2020 response to my letter, which made several dubious claims about your company and failed to answer my questions, was unacceptable. News reports since my initial letter have added to my worries about Clearview, particularly around potential sales to authoritarian regimes and the possibility that Clearview might collect children's images. I write with additional questions based on this new information and to reiterate the need for you to fully reply to my previous inquiry.

Recent reports about Clearview potentially selling its technology to authoritarian regimes raise a number of concerns because you would risk enabling foreign governments to conduct mass surveillance and suppress their citizens. On February 5, 2020, you reportedly told BuzzFeed News that you were "focused on doing business in USA and Canada."[1] Subsequent reporting based on Clearview's internal documents contradicts this statement, alleging that your company has expanded to "at least 26 countries outside the US."[2] Alarmingly, the reporting suggests that Clearview has already provided its software to organizations in countries like Saudi Arabia and the United Arab Emirates, countries governed by authoritarian regimes with poor track records on human rights. The use of sophisticated facial recognition technology is concerning even in a democracy with strong civil liberties, but its export to certain foreign countries could enable mass surveillance and repression of minorities.

---

[1] Ryan Mac, Caroline Haskins, and Logan McDonald, *Clearview AI Wants To Sell Its Facial Recognition Software To Authoritarian Regimes Around The World*, BuzzFeed News (Feb. 5, 2020), https://www.buzzfeednews.com/article/carolinehaskins1/clearview-ai-facial-recognition-authoritarian-regimes-22.

[2] Ryan Mac, Caroline Haskins, and Logan McDonald, *Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA*, BuzzFeed News (Feb. 27, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

Unfortunately, the problem of authoritarian regimes employing facial recognition already exists. As I explained in a letter that I sent to the State Department last year, China exports its surveillance technologies and associated practices to other foreign governments, thereby empowering authoritarianism in different countries.[3] Foreign sales by Clearview would seriously threaten to intensify the problem because of the unprecedented scope of your database of images. Contrary to your claim that Clearview is "like other companies who operate facial recognition software," Clearview is a clear outlier: it scrapes billions of photos from social media sites rather than using relatively limited sets of photos from existing government databases. This is why I am particularly worried that foreign sales of your technology might exacerbate the global trend towards mass surveillance and human rights suppression.

Turning to domestic use of your technology, I am concerned that Clearview might be collecting and processing images of children in violation of federal law. On February 7, 2020, the *New York Times* reported that law enforcement has used Clearview's tools to identify children, including minors as young as 13.[4] In the process of scraping billions of photos from social media to build its database, I fear Clearview may also have indiscriminately collected and processed images of children under 13. To understand why, consider that Facebook, one of the sites that Clearview scraped, was estimated to have millions of underage users even though it officially prohibited children under 13 from using its platform.[5] This raises the troubling possibility that Clearview may have violated the Children's Online Privacy Protection Act,[6] a law I authored, both by scraping children's data and by processing their uploaded images for facial recognition. Federal law requires notice and parental consent to collect and process data from children under 13. In addition, those who receive children's personal information from other websites are expected to have reasonable procedures to protect the confidentiality, security, and integrity of that information.[7] I have grave doubts about Clearview's ability to protect this sensitive data in light of recent reports that hackers successfully stole Clearview's entire client list.[8] Children are a uniquely vulnerable population online, and I am concerned that Clearview may be neglecting its legal obligation to protect kids' privacy.

I am equally disturbed by new reports about other alleged Clearview business practices that may threaten the public's civil liberties and privacy. Investigations have called into question Clearview's claimed successes and uncovered emails from Clearview employees encouraging officers to "run wild" and use Clearview's facial recognition technology on friends, family, and

---

[3] Letter from Senator Ed Markey to Michael R. Pompeo, Secretary of State (June 5, 2019), https://www.markey.senate.gov/imo/media/doc/Letter%20to%20State%20on%20China%20Surveillance%20Exports.pdf.

[4] Kashmir Hill and Gabriel J.X. Dance, *Clearview's Facial Recognition App Is Identifying Child Victims of Abuse*, N.Y. Times (Feb. 7, 2020), https://www.nytimes.com/2020/02/07/business/clearview-facial-recognition-child-sexual-abuse.html.

[5] *CR Survey: 7.5 Million Facebook Users are Under the Age of 13, Violating the Site's Terms*, Consumer Reports (May 10, 2011), https://www.consumerreports.org/media-room/press-releases/2011/05/cr-survey-75-million-facebook-users-are-under-the-age-of-13-violating-the-sites-terms-/.

[6] Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501 – 6506 (2018).

[7] FTC Children's Online Privacy Protection Rule, 16 C.F.R. § 312.8 (2019).

[8] 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.

celebrities.[9] Your own blog suggests that Clearview has private clients outside law enforcement,[10] which is supported by reporting alleging that more than 200 companies, including banks, casinos, and retail stores, have Clearview accounts.[11] Reporting also suggests that Clearview has been developing live facial recognition in surveillance cameras and augmented reality glasses targeted at the private sector.[12] Your website requires that consumers submit sensitive information to have their images deleted from your database. These practices point to a dangerous neglect for privacy at Clearview AI.

Therefore, I respectfully request full responses to my previous questions, available online, [13] as well as answers to the following questions, by March 24, 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?

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.

---

[9] Ryan Mac, Caroline Haskins, and Logan McDonald, *Clearview AI Once Told Cops to "Run Wild" With Its Facial Recognition Tool. It's Now Facing Legal Challenges*, BuzzFeed News (Jan. 28, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-cops-run-wild-facial-recognition-lawsuits. Ryan Mac, Caroline Haskins, and Logan McDonald, *Clearview AI Says Its Facial Recognition Software Identified A Terrorism Suspect. The Cops Say That's Not True*, BuzzFeed News (Jan. 23, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-nypd-facial-recognition.

[10] The Clearview AI Code of Conduct, https://newsroom.clearview.ai/ (last visited Feb. 13, 2020) ("Clearview AI's search engine is available only for law enforcement agencies and **select security professionals** to use as an investigative tool.").

[11] Mac, *supra* note 2.

[12] Caroline Haskins, Ryan Mac, and Logan McDonald, The Facial Recognition Company That Scraped Facebook And Instagram Photos Is Developing Surveillance Cameras, BuzzFeed News (Mar. 2, 2020), https://www.buzzfeednews.com/article/carolinehaskins1/clearview-facial-recognition-insight-camera-glasses.

[13] Letter from Senator Ed Markey to Mr. Hoan Ton-That, Clearview AI (Jan. 23, 2020), https://www.markey.senate.gov/imo/media/doc/Clearview%20letter%202020.pdf.

3. Hackers recently breached Clearview's security and reportedly obtained your entire client list.[14]
    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.

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.

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

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

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?

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?

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

---

[14] 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.

[15] Rebecca Heilweil, *The world's scariest facial recognition software, explained*, Vox (Feb. 11, 2020), https://www.vox.com/recode/2020/2/11/21131991/clearview-ai-facial-recognition-database-law-enforcement.

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

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

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

Thank you for your attention to these requests.

Sincerely,

Edward J. Markey
United States Senator