United States Senate
WASHINGTON, DC 20510

May 21, 2020

Caryn Seidman Becker
Chairman & CEO
CLEAR
650 5th Avenue, 12th Floor
New York, NY 10019

Dear Ms. Seidman Becker:

We write to inquire about data privacy practices and precautions taken for CLEAR's new product, *Health Pass*.

As the nation yields to the unique circumstances brought on by the COVID-19 pandemic, a number of initiatives have been launched with the important goal of allowing our businesses to reopen safely and getting families back to work in a manner consistent with guidance issued by the Centers for Disease Control and Prevention (CDC). Consumers are looking with particular anticipation what steps the travel, entertainment, and food service industries – among others – will take to ensure their safety in a post COVID-19 world.

CLEAR recently announced its new product, *Health Pass*, which would provide consumers with the ability verify one's identity by taking a selfie, and to verify one's health by taking a quiz regarding possible COVID-19 symptoms, and operating separately from efforts around contact tracing. In addition to airports, restaurants, venues, and other places of business will be able to utilize this service by requiring identity and health verification before a customer may board a plane, pass through security, or enter a place of business.

While we appreciate CLEAR's contribution to the discussion of safely reopening our nation's economy, the use of facial recognition technology poses real privacy concerns. Though there are some potential benefits and expediencies, this technology can also be utilized widely and passively in such a way that eludes consumers' awareness, permission, or the ability to opt out. If over or misused, facial recognition technology risks a state of undetectable, constant government surveillance that can track one's movements and associations with organizations such as schools and places of worship.

Equally concerning is the risk associated with the collection of the personally identifiable information of millions of American consumers. On February 26, 2020, Clearview AI, a technology company whose main service provides facial recognition software, announced that it lost its entire client list as a result of a data breach. This breach of a company whose database contains more than three billion photos raises legitimate concern about the heightened risks of potential cyberattacks on facial recognition technology companies.

The COVID-19 pandemic continues to require swift action and innovative solutions to protect the health of Americans and work to save local and national economies, however it should not enable or encourage reliance on technology that could intentionally or unintentionally threaten the privacy and security of millions of consumers, nor should that technology operate without

appropriate protections for its consumers. For these reasons, we request your response to the following questions:

1. What steps has CLEAR taken to ensure the privacy and security of its customers?
2. Does CLEAR collect data concerning their customers? If so, what personally identifiable information or location data is collected, and for how long may this data be retained?
3. Does CLEAR buy, sell or otherwise transfer personally identifiable information or location data to other entities, including both private sector and government agencies?
4. If CLEAR does collect data concerning their customers, does CLEAR claim ownership of any personally identifiable information or location data it may collect?
5. If CLEAR does collect data concerning their customers, does CLEAR provide customers with the ability to delete their personal data or prohibit future collection of personally-identifiable information or location data?
6. Besides expediting identity verification, please explain why facial recognition technology/iris scanning technology are necessary to determine whether an individual has or displays symptoms consistent with COVID-19 (fever, coughing, shortness of breath, etc.)
7. Does CLEAR easily allow for alternative methods to verify identity, such as QR codes?
8. In reaction to a National Institute of Standards and Technology's (NIST) report on the accuracy of facial recognition technology, what steps has CLEAR taken to assess biases in its technology?[1] Has CLEAR submitted its technology to NIST's Face Recognition Vendor Test for an evaluation?

We appreciate your attention to these questions in advance and request a response no later than 30 days from your receipt of this letter.

Sincerely.

Jeffrey A. Merkley
United States Senator

Cory A. Booker
United States Senator

---

[1] National Institute of Standards and Technology. "New Test on the Effect of Masks on Face Recognition Accuracy." May 1, 2020. Available at: https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing