

STATE OF VERMONT

SUPERIOR COURT
CHITTENDEN UNIT

CIVIL DIVISION
DOCKET NO.

STATE OF VERMONT,)
)
Plaintiff,)
)
v.)
)
CLEARVIEW AI, INC.)
)
Defendant.)

VERMONT SUPERIOR COURT
FILED

MAR 10 2020

Chittenden Unit

COMPLAINT

The Vermont Attorney General brings this suit against Clearview AI, Inc. for violations of the Vermont Consumer Protection Act, 9 V.S.A. § 2451 *et seq.* and Vermont’s Fraudulent Acquisition of Data Law, 9 V.S.A. § 2431. For these violations, the Attorney General seeks civil penalties, restitution, injunctive relief, disgorgement, fees and costs, and other appropriate relief.

I. PARTIES, JURISDICTION, AND VENUE

A. Plaintiff

1. The Vermont Attorney General is authorized under the Vermont Consumer Protection Act, 9 V.S.A. § 2458, to sue to enforce the Act’s prohibitions on unfair and deceptive acts and practices in commerce.

2. The Vermont Attorney General is authorized under 9 V.S.A. 2431(b), to enforce Vermont's Fraudulent Acquisition of Data Law in the same manner that it enforces the Vermont Consumer Protection Act.

3. The Vermont Attorney General also has the right to appear in any civil action in which the State has an interest. 3 V.S.A. § 157. The Attorney General has an interest in ensuring that entities that do business in Vermont do so in a lawful manner.

4. Pursuant to 9 V.S.A. § 2460, the Vermont Attorney General conducted an investigation prior to filing this complaint, including the issuance of a Civil Investigative Demand and the review of responsive documents and written responses.

B. Defendant

5. Defendant Clearview AI ("Defendant" or "Clearview") is a Delaware corporation with its principal place of business is located at 214 W. 29th Street, New York, NY 10001.

6. Defendant is engaged in the business of identifying individuals using facial recognition technology applied to photographs.

7. Clearview is registered as a data broker in Vermont's Data Broker Registry, which was created under Vermont's recently enacted data broker law and is maintained by the Secretary of State. 9 V.S.A. § 2446. A data broker is a business that collects and sells or licenses the personal data of individuals with whom it does not have a direct relationship. 9 V.S.A. § 2430.

C. Jurisdiction and Venue

8. The Court has personal jurisdiction over Defendant because it unlawfully acquires data from consumers and business concerns located in Vermont, including in Chittenden County.

9. Venue in this Court is proper because Defendant does business in Chittenden County.

10. This action is in the public interest.

II. FACTUAL BACKGROUND

A. Facial Recognition Technology

11. Facial recognition involves using computers to extract biometric identifiers from photographs based on specific features of the individual's face like relative position, size, or shape of the eyes, nose, cheekbones, and jaw. These identifiers are stored as digital "hashes"¹ in a searchable database in order to quickly identify an individual based on a photograph or video capture.

12. A biometric identifier is a piece of information used to authenticate an individual that is based on that person's physical or behavioral traits. Examples include a fingerprint, DNA mapping, ocular scan, or even an analysis of the way someone walks. Using these identifiers for authentication is very useful for assuring that people are who they claim to be. Biometrics differ from other sorts of authentication, however, in that while an ID badge or password can be changed if

¹ A "hash" is a computerized function that converts a data structure into a unique or near-unique value, which can be more easily searched.

stolen, biometrics cannot. Your fingerprint, DNA, or facial map will stay constant throughout your life.

13. Applying facial recognition to a photograph is entirely different from simply viewing a photograph. Facial recognition extracts a unique, instantly searchable biometric identifier for a person, which that person cannot change absent extreme efforts (like wearing a disguise in public). Once entered into a facial recognition database, the individual loses an enormous measure of anonymity, privacy, and freedom. That individual can now be picked out of a crowd by anyone, be it a government, corporation, or criminal. Every instance of that person's appearance on the internet, be it in the audience of a rally, a mugshot, dining at an intimate restaurant, a reflection in a mirror, or cheering their child at a little league game, can suddenly be pulled together into a single surveillance dossier from which they have no ability to opt out.

14. While all technologies can be beneficial or harmful, businesses and policymakers have been particularly cautious regarding the implementation of facial recognition technology because the potential for misuse and the consequences of such misuse are so dire.

15. Easily accessible facial recognition would permit governments, stalkers, predators, and con artists to instantly identify any stranger and, combined with other readily available data sources, know extensive details about their family, address, workplace, and other characteristics.

16. Even such leading-edge companies with large caches of photographic data as Facebook and Google have declined to make a facial recognition tool commercially available, though they have the capability to do so.

17. In 2011, Google's then-CEO stated of facial recognition, "We built that technology and we withheld it. . . As far as I know, it's the only technology Google has built and, after looking at it, we decided to stop."²

18. In 2016, a Russian start-up called NTech Lab developed FindFace, a facial recognition app very similar to the product at issue in this case, and collected the photographs of 200 million users from VKontakte, a Russian Social network. Concerns were raised then that something similar would happen here, but it was not believed at the time that such technology would work on American social media companies due to their stronger privacy controls.³

19. Several studies have found that facial recognition technologies are inaccurate, particularly when identifying people of color. A report issued in December 2019 by the National Institute of Standards and Technology ("NIST"), the federal agency responsible for promoting standards, found that the likelihood of

² Blanca Bosker, *Facial Recognition: The One Technology Google Is Holding Back*, Huffington Post, Jun. 1, 2011, https://webcache.googleusercontent.com/search?q=cache:MwDlXjKEg2oJ:https://www.huffpost.com/entry/facial-recognition-google_n_869583 (last visited March 9, 2020).

³ Jonathan Frankle, *How Russia's New Facial Recognition App Could End Anonymity*, The Atlantic, May 23, 2016, <https://www.theatlantic.com/technology/archive/2016/05/find-face/483962/> (last visited March 9, 2020).

false positives was from ten to 100 times more likely when the subject was African American or Asian.⁴ This report reviewed 189 algorithms from 99 developers.

20. Law enforcement's use of a massive facial recognition database, like the one described below, essentially puts every individual in that database, whether they had ever done anything wrong or not, into a permanent, inescapable virtual lineup or "rogues gallery" accessible for any reason at any time.

21. Several states have enacted or are considering moratoriums on the use of facial recognition. California banned the use of facial recognition scanners in police body cameras until 2023. Similar legislation is pending in Massachusetts, Michigan, New Hampshire, New York, Utah, and Washington.⁵

22. Eight municipalities have gone so far as to ban the use of facial recognition technology by their law enforcement agencies: San Francisco, Oakland, Berkeley and Alameda, California, and Somerville, Northampton, Cambridge, and Brookline, Massachusetts.⁶

23. The Human Rights Council of the United Nations has identified electronic surveillance, including facial recognition technology, as a threat to the civil rights of citizens. Specifically, it finds: "In environments subject to rampant illicit surveillance, the targeted communities know of or suspect such attempts at surveillance, which in turn shapes and restricts their capacity to exercise the rights

⁴ National Institute of Standards and Technology, U.S. Department of Commerce, Gother, P. *et al.*, Face Recognition Vendor Test Part 3: Demographic Effects, (Dec. 2019).

⁵ Fight for the Future, Interactive Map, <https://www.banfacialrecognition.com/map/> (last visited March 9, 2020).

⁶ *Id.*

to freedom of expression, association, religious belief, culture and so forth. In short, interference with privacy through targeted surveillance is designed to repress the exercise of the right to freedom of expression.”⁷

B. Clearview AI

24. Clearview is a small startup company that developed facial recognition technology and, using “screen scraping” technology (addressed below) amassed a database of three *billion* photographs.

25. Clearview collected the photographs by scouring millions of websites. It has commercialized these photographs via a service that allows the customer to upload a photograph in order to instantly identify the individual through facial recognition matching.⁸

26. Clearview was founded by Hoan Ton-That, a California resident.

27. Prior to creating Clearview, Ton-That was involved in other companies including ViddyHo.com, an alleged phishing⁹ site which tricked users into sharing access to their gmail account so that it could generate spam to the users’ contacts.¹⁰

⁷ United Nations Human Rights Council, Forty-first session, 24 June–12 July 2019, Agenda item 3, (Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression). <http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/41/35&Lang=E> (last visited March 9, 2020).

⁸ Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. Times, Jan. 18, 2020, <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html> (last visited March 9, 2020).

⁹ “Phishing” is the fraudulent attempt to steal information like passwords and financial information by sending electronic communications that are disguised as requests from legitimate and trusted entities.

¹⁰ Owen Thomas, *The person behind a privacy nightmare has a familiar face*, S.F. Chronicle, Jan. 22, 2020, <https://www.sfchronicle.com/business/article/The-person-behind-a-privacy-nightmare-has-a-14993625.php> (last visited Mar. 9, 2020); *see also* Gabriel Snyder,

28. Ton-That also founded Fastforwarded.com, an alleged phishing site which tried to fraudulently extract passwords from users.¹¹

29. The general public first learned of Clearview in January 2020 as the result of an exposé by The New York Times (“NYT”).¹²

30. Clearview states on its website: “Clearview’s app is **NOT** available to the public. While many people have advised us that a public version would be more profitable, we have rejected the idea. Clearview exists to help law enforcement agencies solve the toughest cases, and our technology comes with strict guidelines and safeguards to ensure investigators use it for its intended purpose only.” (emphasis in original)¹³

31. According to news reports, this is untrue. Clearview has allegedly provided access to its app to numerous for-profit corporations including Best Buy, Macy’s, Kohl’s, Walmart, Albertsons, Rite Aid, AT&T, Verizon, T-Mobile, Wells Fargo, Bank of America, the Las Vegas Sands Casino, Madison Square Garden, the NBA, Equinox Fitness, and more than fifty universities, among others. Clearview has reportedly made the app available to investors for use in public spaces,¹⁴ and

ViddyHo Worm Sweeping Through IM, Gawker, Feb. 24, 2009, <https://gawker.com/5159815/viddyho-worm-sweeping-through-im> (last visited Mar. 9, 2020).

¹¹ Owen Thomas, ‘Anarcho-Transexual’ Hacker Returns with New Scam Site, Gawker, Mar. 10, 2009, <https://gawker.com/5167506/anarcho-transexual-hacker-returns-with-new-scam-site> (last visited Mar. 9, 2020)

¹² *Supra note 8*.

¹³ Clearview AI Newsroom, <https://newsroom.clearview.ai/> (last visited Mar. 9, 2020).

¹⁴ Kashmir Hill, *Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich*, *N.Y. Times*, Mar. 5, 2020, <https://www.nytimes.com/2020/03/05/technology/clearview-investors.html> (last visited Mar. 9, 2020).

reporters also claimed that the app had been made publicly available such that the reporters could download it.¹⁵ Clearview has also allegedly provided access to governments or businesses in up to 27 countries, including Saudi Arabia and the United Arab Emirates, two countries with a history of silencing dissidents.¹⁶

32. Even within law enforcement agencies, Clearview has not limited the use of its app to authorized users. On February 20, 2020, the Chief of the Raleigh, North Carolina police department acknowledged in a memo that despite having authorized three employees to use the app, Clearview had granted access to additional individuals through “an email regarding an invitation, user referral or free trial from the company.”¹⁷

33. Further, in a November 2019 email to a police lieutenant in Green Bay, Wisconsin, Clearview stated:

“Have you tried taking a selfie with Clearview yet? . . . It’s the best way to quickly see the power of Clearview in real time. Try your friends or family. Or a celebrity like Joe Montana or George Clooney.

Your Clearview account has unlimited searches. So feel free to run wild with your searches. Test Clearview to the limit and see what it can do. The photos you search with Clearview are **always** private and

¹⁵ Dell Cameron *et al.*, *We Found Clearview AI's Shady Face Recognition App*, Gizmodo, Feb. 27, 2020, <https://gizmodo.com/we-found-clearview-ais-shady-face-recognition-app-1841961772?rev=1582861547126> (last visited Mar. 9, 2020).

¹⁶ Ryan Mac *et al.*, *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> (last visited Mar. 9, 2020).

¹⁷ Joedy McCreary, *Raleigh Police: Face ID company offered free trials to unauthorized employees*, CBS 17, Feb. 25, 2020, <https://www.cbs17.com/news/digital-investigations/raleigh-police-face-id-company-offered-free-trials-to-unauthorized-employees/> (last visited Mar. 9, 2020).

never stored in our proprietary database, which is totally separate from the photos you search.”¹⁸

(Emphasis in original.)

34. In other words, Clearview encouraged police officers to use the tool on innocent citizens; and when someone uploads a photograph in order to find a match, the uploaded photograph and a record of that upload is not kept.

35. NYT reporter Kashmir Hill reported that, in connection with her investigation, she asked various police departments to run her own photograph through Clearview’s app. Her image did not generate a match, but after police departments performed the search, they were contacted by Clearview and told not to speak to the NYT. Hill concluded that this was because Clearview knew of the NYT investigation and was both monitoring the law enforcement searches and manipulating the results.¹⁹

36. When Hill confronted Mr. Ton-That with this conclusion, he claimed that this was a “software bug,” which is the same explanation he used to explain the phishing virus developed by his prior enterprise, ViddyHo.com.²⁰

¹⁸ Ryan Mac *et al.*, *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> (last visited Mar. 9, 2020)

¹⁹ See *supra* note 8, see also *‘The Daily’: The End of Privacy as We Know It?* N.Y. Times Podcast, Feb. 10, 2020, <https://www.nytimes.com/2020/02/10/podcasts/the-daily/facial-recognition-surveillance.html> (last visited Mar. 9, 2020).

²⁰ *Id.*

C. Screen Scraping

37. Screen scraping is a term for sending automated scripts or other processes, sometimes called “spiders,” “web scrapers” or “crawlers” to collect information throughout the internet, such as downloading photographs.

38. When a photograph is uploaded to a website, it carries with it various limitations on use based on the Terms of Service of those websites, common law, property rights, and even the reasonable expectations of the photographer and the individual in the image. The fewest limitations may exist on a photograph that is in the public domain, or that has been released with a specific kind of license (often called a creative commons license) that essentially releases all limitations on use of the photograph.

39. If a photograph is uploaded to Facebook and the privacy settings are set to “public,” that photograph is subject to Facebook’s Terms of Service (which prohibit screen scraping). It can be *viewed* by any individual human being on Facebook’s platform, but it may not be screen scraped because that would violate the terms of service. Social media websites deploy administrative and technological safeguards to prevent screen scraping. The uploaded photograph will not show up in Google Image Search, because although Google Image Search deploys spiders, those algorithms respect the Terms of Service of the websites that they visit.

40. Clearview has claimed to only collect “publicly available” photographs, but this has not been independently verified.

41. Furthermore, the term “publicly available” does not have any meaning in the manner used by Clearview, as even though a photograph is being displayed on a certain social media website, it is being displayed subject to all of the rights and agreements associated with the website, the law, and reasonable expectations. One of those expectations was *not* that someone would amass an enormous facial-recognition-fueled surveillance database, as the idea that this would be permitted in the United States was, until recently, unthinkable.

42. Thus, when an individual uploads a photograph to Facebook for “public” viewing, they consent to a human being looking at the photograph *on Facebook*. They are *not* consenting to the mass collection of those photographs by an automated process that will then put those photographs into a facial recognition database. Such a use violates the terms under which the consumer uploaded the photograph, which the consumer reasonably expects will be enforced.

43. Several major websites, including Google, Facebook, Twitter, YouTube, Venmo, and LinkedIn have sent cease-and-desist or similar letters to Clearview accusing it of violating their Terms of Service by using screen scraping to collect photographs posted on their platforms.²¹ Some of the Terms of Service on these websites include:

²¹ *Google, YouTube, Venmo and LinkedIn send cease-and-desist letters to facial recognition app that helps law enforcement*, CBS News, Feb. 5, 2020, <https://www.cbsnews.com/news/clearview-ai-google-youtube-send-cess-and-desist-letter-to-facial-recognition-app/> (last visited Mar. 9, 2020).

- a. Facebook: “You may not access or collect data from our Products using automated means (without prior permission) or attempt to access data you do not have permission to access.”²²
- b. Google: “You may not copy, modify, distribute, sell, or lease any part of our Services” and “You may not use content from our Services unless you obtain permission from its owner or are otherwise permitted by law.”²³
- c. Twitter: “you may not . . . access or search or attempt to access or search the Services by any means (automated or otherwise) other than through our currently available published interfaces that are provided by Twitter” and explicitly stating that “scraping the Services without the prior consent of Twitter is expressly prohibited.”²⁴
- d. YouTube: a person may not “access the Service using any automated means (such as robots, botnets or scrapers) except . . . with YouTube’s prior written permission” and may not “collect or harvest any information that might identify a person, unless permitted by that person.”²⁵
- e. LinkedIn: a user agrees that they “will *not*. . . use software, devices, scripts, robots or any other means or processes (including crawlers, browser plugins and add-ons or any other technology) to scrape the Services or otherwise copy profiles and other data from the Services.”²⁶ [emphasis in original]
- f. Venmo: “you must not . . . use any robot, spider, or other automatic device, or manual process to monitor or copy our websites without

²² Facebook Terms of Service, Section 3, item 2, *available at*: <https://www.facebook.com/legal/terms> (last visited Mar. 9, 2020).

See also Facebook “Automated Data Collection Terms” at ¶ 2 (“You will not engage in Automated Data Collection without Facebook’s express written permission.”), *available at*: https://www.facebook.com/apps/site_scraping_tos_terms.php (last visited Mar. 9, 2020).

²³ Google Terms of Service, *available at*: <https://policies.google.com/terms?hl=en-US> (last visited Mar. 9, 2020).

²⁴ Twitter User Agreement, section 4, *available at*: <https://twitter.com/en/tos> (last visited Mar. 9, 2020).

²⁵ YouTube Terms of Service, “Your Use of Service, Permissions and Restrictions” ¶¶ 3-4, *available at*: <https://www.youtube.com/static?template=terms> (last visited Mar. 9, 2020).

²⁶ LinkedIn User Agreement, section 8.2(b), *available at*: <https://www.linkedin.com/legal/user-agreement> (last visited Mar. 9, 2020).

our prior written permission”; “you must not . . . infringe our or any third party’s . . . rights of publicity or privacy”; and “you must keep” all Venmo customer information “confidential and only use it in connection with the Venmo services.”²⁷

44. When a consumer posts a photograph on a website, they retain exclusive rights to the usage of that photograph unless they have otherwise granted a subset of those rights through Terms of Service, license agreement, or other means. Screen scraping, as Clearview used it, resulted in the collection of billions of photographs, without the permission of their owners, for a clearly commercial, for-profit use.

45. It should be recognized that not all images posted on the web were placed there by the individual pictured with the intent of publicizing it to the world. Many images that are posted on the open web were not acceded to by the individual pictured. It is not uncommon for website coding errors to make photographs available to the public accidentally, even if for the limited time necessary for Clearview’s spiders to capture them. Or, one might be photographed at a private party or intimate dinner in a restaurant and have their photograph posted on the web. For example, one website (Classmates.com) has scanned hundreds of thousands of school yearbooks dating back over a century and has posted those photographs online.²⁸ No one who sat for their high school senior yearbook photo in

²⁷ Venmo User Agreement, “Restricted Activities,” *available at*: <https://venmo.com/legal/user-agreement/#restricted-activities> (last visited Mar. 9, 2020).

²⁸ <https://www.classmates.com/yearbooks/> (last visited Mar. 9, 2020).

1985 consented to have their image collected, scanned, analyzed, and posted to a facial recognition database in 2020.

46. Some spiders also access “non-public” information by circumventing security and authorization technologies using prohibited operations similar to the technologies that Clearview’s founder is alleged to have used in prior businesses.

D. Collecting Data of Minors

47. Data brokers that sell Vermonters’ data must register annually with the Vermont Data Broker Registry and provide certain information.²⁹

48. Clearview did not register with Vermont’s registry in 2019, but it did on January 14, 2020, four days before the initial NYT article was published.

49. Clearview responded “yes” to the question, “Does the data broker have actual knowledge that it possesses the brokered personal information of minors.”

50. In response to the follow-up question, “If so, provide a statement detailing the data collection practices, databases, sales activities, and opt-out policies that are applicable to the brokered personal information of minors,”

Clearview stated:

“Clearview AI Inc. collects publicly available images. This collection includes publicly available images of minors. We provide collected images in a searchable format to users. We actively work to remove all images of California-resident minors from all datasets. Clearview AI, Inc. processes all opt-out requests in a manner compliant with the relevant local laws, including opt-out requests related to minors.”³⁰

²⁹ 9 V.S.A. § 2466.

³⁰ *Id.*

51. There is no statute in force in Vermont that would specifically require Clearview to honor an opt-out request made on behalf of a Vermont minor. Further, the Attorney General's investigation has revealed that Clearview does not yet have the capability to remove individuals by geographic region or age.

52. There are strong social norms against the type of mass-collection and facial recognition implemented by Clearview, as evidenced by the facts that up until now, United States companies like Google have refused to develop such technology for general public use; that the Russian FindFace app was never adopted in the United States; and the outrage expressed in the media over the revelation that Clearview exists. These sorts of expectations are even stronger for the mass-collection of the photographs of children.

53. Given these norms, consumers have been uploading their photographs to the internet under the reasonable expectation that their photographs and those of their children would not be collected and added to a massive facial recognition database.

54. Clearview has made no attempt to obtain the consent of any adult prior to collecting and applying facial recognition to their photograph, or any parent or guardian prior to collecting the information of their children.

55. Minors cannot consent to having their photographs added to a facial recognition database. However, once captured by Clearview, they are entered into this surveillance system for the rest of their lives.

E. Claims Made by Clearview

Privacy Rights

56. In its Privacy Policy posted on its website, Clearview states the following regarding consumers' privacy rights:

What are your data protection rights?

Clearview AI would like to make sure you are fully aware of all your data protection rights. Users and members of the public are entitled to the following:

The right to access - You have the right to request that Clearview AI provides you with copies of your personal data.

The right to rectification - You have the right to request that Clearview AI correct any information that you believe is inaccurate. You also have the right to request Clearview AI complete information you believe is incomplete.

The right to erasure - You have the right to request that we erase your personal data under certain conditions.

The right to object to processing - You have the right to object to Clearview AI's processing of your personal data under certain conditions.

The right to data portability - You have the right to request that Clearview AI transfer the data that we have collected to you or to another organization at your consent.

Requests to exercise data protection rights can be submitted here to privacy-requests@clearview.ai. (see below for further instructions)

These rights are subject to limitations that vary by jurisdiction. We will honor such requests, withdrawal or objection as required under applicable data protection rules but these rights are not absolute: they do not always apply and exemptions may be engaged. Clearview does require that persons requesting the sharing or deletion of their personal data provide us with information to verify their identity and to facilitate the processing of data requests. While most of this information is deleted after the completion of the request, Clearview is required to retain some of this

information to maintain a record of data rights requests. If we do not comply with your request, we will explain why.

(emphasis in original)

57. These “data protection rights” describe the express rights of citizens of the European Union as laid out under a recently enacted law, the General Data Protection Regulation (“GDPR”), which applies to all companies doing business in the European Union.³¹ United States citizens, however, do not have such explicit rights of general applicability under current law. There is no U.S. federal privacy law of general applicability, other than the protections of the Federal Trade Commission Act’s prohibition of Unfair and Deceptive Acts and Practices, that applies to a company like Clearview. The only state law that comes close to providing these rights is the California Consumer Privacy Act (“CCPA”), Cal. Civ. Code §§ 1798.100-1798.199, which only protects the rights of California citizens.

58. Vermont, and forty-eight other states, do not have laws that provide these explicit “data protection rights.” By stating that “users and members of the public are entitled” to these rights, and later noting that these “rights are subject to limitations that vary by jurisdiction,” Clearview creates a reasonable belief in any Vermont consumer who is not a privacy law scholar that they can take some action to protect their privacy with regard to data stored in Clearview’s databases, if that person even knew that the database was being amassed.

³¹ Regulation (EU) 2016/679 (General Data Protection Regulation), <https://gdpr-info.eu/> (last visited Mar. 9, 2020).

59. Clearview's Privacy Policy goes on to state: "We are not allowed to process personal data if we do not have a valid legal ground. Therefore, we will only process personal data if . . . the processing is necessary for the legitimate interests of Clearview, and does not unduly affect your interests or fundamental rights and freedoms."

60. This is untrue. Clearview's processing does very much unduly affect consumers' interests and fundamental rights and freedoms.

Strength of Data Security

61. In its Privacy Policy, Clearview states: "We use a variety of security technologies and procedures to help protect all of the personal information that we process, whether from users or from the Internet, against unauthorized access, use or disclosure. We secure all personal information that we store on computer servers in a controlled, secure environment, protected from unauthorized access, use or disclosure. All personal information is protected using appropriate physical, technical and organizational measures."³²

62. This statement would lead a reasonable consumer who is not technologically sophisticated to believe that the personal data Clearview stores is completely secure, despite the impossibility of such a claim.

63. To date, Clearview has not demonstrated to the Attorney General's Office or otherwise that it has implemented reasonable data security measures.

³² *Id.*

64. On February 26, 2020, Clearview experienced a data breach in which Clearview's client list was stolen.³³

65. The February data breach demonstrates the vulnerability of Clearview's data security despite its prior representations.

66. In the wake of the breach, Clearview issued the statement, "Unfortunately, data breaches are part of life in the 21st century."³⁴

67. This statement is true. Given the rash of data security breaches in the past decade, including successful attacks by state actors like China, Russia, and North Korea on sophisticated organizations like Equifax, Sony, the U.S. Office of Personnel Management, and the National Security Agency, it would be irresponsible to create a database like Clearview has, the breach of which would cause extraordinary injury to the nonconsenting consumers being tracked, absent very strong data security.³⁵

68. Clearview has failed to provide a level of data security proportional to the sensitivity of the data that Clearview is collecting.

³³ 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> (last visited Mar. 9, 2020).

³⁴ *Id.*

³⁵ Federal Trade Commission, Statement of Commissioner Rohit Chopra Joined by Commissioner Rebecca Kelly Slaughter, Mar. 2, 2020, https://www.ftc.gov/system/files/documents/public_statements/1567795/final_statement_of_rchopra_re_safeguards.pdf (last visited Mar. 9, 2020); *see also* Charlie Warzel, *Chinese Hacking Is Alarming. So Are Data Brokers.*, N.Y. Times, Feb. 10, 2020, <https://www.nytimes.com/2020/02/10/opinion/equifax-breach-china-hacking.html> (last visited Mar. 9, 2020).

Code of Conduct

69. In its “Clearview User Code of Conduct,” under “Appropriate and Authorized Use” Clearview states:

Users may only use the Clearview app for legitimate law enforcement and security purposes. All use of the Clearview app must be authorized by a supervisor employed by the user’s organization.

Users may not use the Clearview app for personal purposes, or for any purposes which are not authorized and directed by the user organization’s supervisors.³⁶

70. This statement contradicts Clearview’s private marketing admonition to use the app on friends and family and to “feel free to run wild with your searches.” *Supra* ¶ 33.

Accuracy of Matching Technology

71. Clearview has claimed, without evidence and without applying a standard benchmark, an accuracy rate of 98.6% to 99.6% for matching photographs using its technology. It has compared these rates to those of its competitors Tencent (83.3%) and Google (70.4%), which were obtained through a widely used facial recognition benchmark called the MegaFace test, implemented by the University of Washington.³⁷

³⁶ Clearview AI User Code of Conduct, https://blog.clearview.ai/code_of_conduct.pdf (last visited Mar. 9, 2020).

³⁷ Ryan Mac *et al.*, *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> (last visited Mar. 9, 2020).

72. Clearview has claimed on its website that “An independent panel of experts rated Clearview 100% accurate across all demographic groups according to the ACLU’s facial recognition accuracy methodology.” This claim was removed after the American Civil Liberties Union responded that Clearview had not properly applied their methodology and that the statement was “absurd on many levels” and amounted to “manufacturing endorsements.”³⁸

73. The only entity that provides public testing of facial recognition technology is NIST, through its Face Recognition Vendor Test.³⁹ Clearview has not provided its matching algorithm to NIST in order to be tested.

Helping Solve Investigations

74. Clearview has made numerous claims regarding its assistance in solving New York Police Department (NYPD) cases:⁴⁰

- a. Clearview claimed in a marketing presentation to law enforcement agencies to have assisted the NYPD in identifying within seconds a terrorism suspect who placed devices made to look like bombs in a New York City subway station.
- b. One marketing flyer stated: “On September 24, 2018, *The Gothamist* published a photo of a man who assaulted two individuals outside a

³⁸ Caroline Haskins *et al.*, *The ACLU Slammed A Facial Recognition Company That Scrapes Photos From Instagram And Facebook*, BuzzFeed News, Feb. 10, 2020, <https://www.buzzfeednews.com/article/carolinehaskins1/clearview-ai-facial-recognition-accurate-aclu-absurd> (last visited Mar. 9, 2020).

³⁹ <https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt> (last visited Mar. 9, 2020).

⁴⁰ *Supra* note 37.

bar in Brooklyn, NY. . . Using Clearview, the assailant was instantly identified from a large-scale, curated image database and the tip was delivered to the police, who confirmed his identity.”

c. Clearview also claimed to have assisted the NYPD with an alleged December 2018 groping incident on the New York City subway.

75. The NYPD has denied that Clearview was used in any of these cases.⁴¹

VIOLATIONS OF THE LAW

COUNT ONE

Unfair Acts and Practices in Violation of 9 V.S.A. § 2453

76. The State realleges and incorporates by reference each of the allegations contained in all paragraphs of this Complaint as though fully alleged herein.

77. Defendant has engaged and is continuing to engage in unfair acts and practices in commerce, in violation of the Vermont Consumer Protection Act, 9 V.S.A. § 2453(a), which offend public policy as it relates to the privacy of Vermont’s consumers; are immoral, unethical, oppressive and unscrupulous; and cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

⁴¹ *Id.*

78. Defendant's unfair acts include:
- a. Screen scraping billions of photographs without the consent of their owners, many of which had been uploaded subject to Terms of Service of websites which limited how they could be used;
 - b. Collecting, storing, analyzing and distributing the photographs of minors without the consent of their parents or guardians;
 - c. Invading the privacy of consumers;
 - d. Failing to provide adequate data security for the data it has collected;
 - e. Exposing consumers' sensitive personal data to theft by foreign actors and criminals;
 - f. Violating the civil rights of consumers by chilling their freedoms of assembly and political expression;
 - g. Violating the rights that consumers have as to the display and distribution of their photographs and other property rights; and
 - h. Exposing citizens to the threat of surveillance, stalking, harassing, and fraud.

COUNT TWO
Deceptive Acts and Practices in Violation of 9 V.S.A. § 2453

79. The State realleges and incorporates by reference each of the allegations contained in all paragraphs of this Complaint as though fully alleged herein.

80. Defendant engaged in and is continuing to engage in deceptive acts and practices in commerce, in violation of the Vermont Consumer Protection Act, 9 V.S.A. § 2453(a), by making material misrepresentations that are likely to deceive a reasonable consumer. The meaning ascribed to Defendant's claims herein is reasonable given the nature of those claims.

81. Defendant's deceptive acts include making materially false or misleading statements regarding:

- a. the ways that Vermont consumers can assert their privacy rights to opt out of the product;
- b. that Clearview's processing of consumers' personal data does not unduly affect their interests or fundamental rights and freedoms;
- c. the strength of its data security;
- d. that the product is only used by law enforcement agencies and is not publicly available;
- e. that it removes consumers from its database to comply with relevant laws;
- f. the accuracy of its facial recognition matching product; and
- g. its success in assisting law enforcement investigations.

COUNT THREE
Acquisition and Uses of Brokered Personal Information in
Violation of 9 V.S.A. § 2431

82. The State realleges and incorporates by reference each of the allegations contained in all paragraphs of this Complaint as though fully alleged herein.

83. Vermont's Fraudulent Acquisition of Data Law prohibits the acquisition of "brokered personal information" through fraudulent means, 9 V.S.A. § 2431(a)(1).

84. Violation of Vermont's Fraudulent Acquisition of Data Law is considered an unfair and deceptive act in commerce.

85. "Brokered personal information" includes biometric data used to identify a consumer. 9 V.S.A. § 2430(1)(A)(vi).

86. Defendant's use of screen scraping technology constitutes fraudulent acquisition of brokered personal information in violation of Vermont's Fraudulent Acquisition of Data Law, 9 V.S.A. § 2431(a)(1).

WHEREFORE, Plaintiff State of Vermont respectfully requests that the Court enter judgment in its favor and the following relief:

1. A judgment determining that Defendant has violated the Vermont Consumer Protection Act;
2. A judgment determining that Defendant has violated Vermont's Fraudulent Acquisition of Data Law;
3. A permanent injunction prohibiting Defendant from engaging in the unfair and deceptive acts and practices identified herein;
4. A permanent injunction prohibiting Defendant from engaging in prohibited acquisitions and uses of brokered personal information;

5. A permanent injunction requiring that Defendant delete all Vermont consumers' photographs and facial recognition data from their databases;

6. A permanent injunction requiring that Defendant refrain from collecting Vermont consumers' photographs;

7. A judgment requiring Defendant to provide restitution to all Vermont consumers whose photographs were collected and analyzed by Defendant;

8. A judgment requiring Defendant to disgorge all profits obtained as a result of their violations of the Vermont Consumer Protection Act;

9. A judgment requiring Defendant to disgorge all profits obtained as a result of their violations of Vermont's Fraudulent Acquisition of Data Law;

10. Civil penalties of \$10,000 for each violation of the Vermont Consumer Protection Act;

11. Civil penalties of \$10,000 for each violation of Vermont's Fraudulent Acquisition of Data Law;


12. The award of investigative and litigation costs and fees to the State of Vermont; and

13. Such other and further relief as the Court may deem appropriate.

Dated: March 10, 2020

STATE OF VERMONT

THOMAS J. DONOVAN JR.
ATTORNEY GENERAL

By: 
Ryan Kriger
Justin Kolber
Jill Abrams
Assistant Attorneys General
Office of Attorney General
109 State Street
Montpelier, Vermont 05609
ryan.kriger@vermont.gov
justin.kolber@vermont.gov
jill.abrams@vermont.gov
(802) 828-3170