IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

JOHN McPHERSON, Individually and on Behalf of All Others Similarly Situated, Plaintiff, v. CLEARVIEW AI, INC., a Delaware Corporation; HOAN TON-THAT, an Individual; RICHARD SCHWARTZ, an Individual; and DOES 1 through 10, inclusive, Defendants.	Case No. _____ CLASS ACTION **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff John McPherson ("Plaintiff"), by his attorneys, brings this action individually and on behalf of all others similarly situated (the "Class") against Defendants Clearview AI, Inc. ("Clearview"), Hoan Ton-That ("Ton-That"), Richard Schwartz ("Schwartz"), and Does 1 through 10, inclusive (collectively, "Defendants"). Plaintiff makes the following allegations upon information and belief (except those allegations as to the Plaintiff or his attorneys, which are based on personal knowledge), based upon an investigation that is reasonable under the circumstances, which allegations are likely to have evidentiary support after a reasonable opportunity for further investigation and/or discovery.

NATURE OF ACTION

1. The disturbing conduct at issue in this Complaint was highlighted in a letter by U.S Senator Edward J. Markey ("Senator Markey") to Clearview about its use of technology to collect, generate, and sell consumers' biometric information without their consent:

> "Widespread use of your technology could facilitate dangerous behavior and could effectively destroy individuals' ability to go about their daily lives anonymously."
>
> "The ways in which this technology could be weaponized are vast and disturbing."[1]

2. As warned by Senator Markey, "[a]ny technology with the ability to collect and analyze individuals' biometric information has alarming potential to impinge on the public's civil liberties and privacy." *Id.* Indeed, Defendants' use of Clearview's technology does just that and violates Illinois's privacy protection statute, among other laws.

3. Without notice or consent, Clearview illicitly "scraped" hundreds, if not thousands or more, websites, such as Facebook, Twitter, and Google, for over three billion images of consumers' faces.[2] Clearview's automated scraping for images violated the policies of websites like Facebook and Twitter, the latter of which specifically prohibits scraping to build facial recognition databases. Unlawfully, Defendants stored billions of scraped images of faces in Clearview's database, used its facial recognition software to generate biometric information (aka a "Faceprint") to match the face to identifiable information, and then sold access to the database to third-party entities and agencies for commercial gain.

4. In clear violation of multiple privacy laws, Clearview sold for a profit access to billions of consumers' Faceprints to law enforcement agencies and private companies across the country, including in New York and Illinois. Consumers did not receive notice of this violation of their privacy rights, and they certainly have not consented to it – in writing or otherwise.

---

[1] Letter from Edward J. Markey, U.S. Senator for Massachusetts to Hoan Ton-That, Founder and Chief Executive Officer of Clearview AI, Inc. (Jan. 23, 2020), https://www.markey.senate.gov/imo/media/doc/Clearview%20letter%202020.pdf ("Markey Letter").

[2] Web "scraping" (aka web harvesting or web data extraction) is data scraping used for extracting data from websites. It is a form of copying in which specific data is gathered/fetched and copied/processed from the web, typically into a central local database or spreadsheet, for later use.

Clearview and its customers, including law enforcement and each of their employees, staff, and any number of other people, may be able to access billions of consumers' identities, social connections, and other personal details based on the Faceprint created and sold by Clearview. As acknowledged by the co-director of the High-Tech Law Institute at Santa Clara University, the "weaponization possibilities of this are endless." Imagine a rogue employee of one of Clearview's customers who wants to stalk potential romantic partners, a foreign government using it to discover information to use to blackmail key individuals, or law enforcement agencies prying into the private lives of citizens with no probable cause or reasonable suspicion. The "dystopian future" of a mass surveillance state has arrived with the erosion of privacy for billions of people, and Clearview is at the helm.

5. To redress the harms suffered, Plaintiff, individually and on behalf of the Class and sub-classes (as defined herein) brings claims for: (a) violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq*. ("BIPA") (on behalf of Plaintiff and the BIPA Class against all Defendants); (b) unjust enrichment (aka "restitution" or "quasi-contract") (on behalf of Plaintiff and the Unjust Enrichment Class against Defendant Clearview); and (c) relief under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq*., on behalf of the Class.[3]

JURISDICTION

6. This Court has original jurisdiction over this action under 28 U.S.C. §1332(a), as well as the Class Action Fairness Act of 2005, 28 U.S.C. §1332(d)(2), as to the named Plaintiff and every member of the Class, because the proposed Class contains more than 100 members, the aggregate amount in controversy exceeds $5 million, and Class members reside in and are citizens

[3] The sub-classes are defined in ¶¶52-53 below.

of a state different from Defendants. The Court has supplemental jurisdiction over Plaintiff's state law claims pursuant to 28 U.S.C. §1367(a).

7. This Court has personal jurisdiction over Plaintiff because Plaintiff submits to the Court's jurisdiction for the purpose of this Complaint. This Court has personal jurisdiction over Clearview because it resides in and is a citizen of New York, New York. Clearview has done a substantial amount of business in New York, including in this District; is authorized to conduct business in New York, including in this District; and/or has intentionally availed itself of the laws and markets of this District through the use, promotion, sale, marketing, and/or distribution of its products and services at issue in this Complaint. Clearview's liability to Plaintiff and the Class arises from and relates to Clearview's conduct within the state of New York. As set forth, *infra*, Clearview acted within New York to collect the biometric information of Plaintiff and persons throughout the United States. Clearview put this biometric information, collected within the state of New York, to commercial use throughout the United States, including within the states of New York and Illinois. Further, Clearview harvests the biometric information of Plaintiff and persons throughout the United States, wherever that biometric information is harvested, and subsequently put that biometric information to commercial use within the states of, among others, New York and Illinois. Thus, Clearview has purposefully availed itself of the benefits and protections of the state of New York in conducting its unlawful enterprise, which purposeful availment constitutes sufficient minimum contacts with the state of New York that the exercise of personal jurisdiction over Clearview with regard to the claims of Plaintiff and the Class does not violate Due Process.

8. This Court has personal jurisdiction over Defendants Ton-That and Schwartz because, as set forth in more detail below, they conspired with Clearview and the Co-Conspirators (defined herein) to further the illegal scheme alleged in this Complaint, which directly targeted

and impacted thousands, if not millions, of New York residents and citizens, including in this District. Defendants Ton-That and Schwartz consented to, authorized, and directed the business conduct at issue in New York, including in this District and have availed themselves of the laws and markets of this District.

9. Venue is proper in this District pursuant to 28 U.S.C. §1391 because Clearview maintains its corporate headquarters and principal place of business in this District. Likewise, venue is proper in this District because a substantial part of the events or omissions giving rise to the claims occurred in this District. Venue is also proper under 18 U.S.C. §1965(a) because Clearview transacts a substantial amount of its business in this District. Alternatively, venue is proper under 28 U.S.C. §1391(b)(3) because this Court has personal jurisdiction over Defendants.

THE PARTIES

Plaintiff John McPherson

10. Plaintiff John McPherson ("McPherson") is a natural person and over the age of 18. Plaintiff McPherson is, and at all relevant times has been, a resident and citizen of Quincy, Illinois.

11. Throughout the relevant period of this Complaint, numerous photographs that include images of Plaintiff McPherson's face were uploaded to various internet-based platforms and websites, including Facebook, Twitter, Instagram, Google, Venmo, and/or YouTube.

12. Clearview "scraped" images of Plaintiff's face from internet-based websites in violation of several of the websites' terms of use and stored them in its database. Based on information and belief, in order to scrape Plaintiff's image, Clearview's web scraper harvested information stored on servers in various states, including New York and Illinois, among others. Clearview also targeted companies that are at home in the state of New York and Illinois, among others, to perform its unlawful scraping. Clearview's software application then applied facial

recognition software to the images of Plaintiff's face, calculated his unique physical characteristics, and generated a biometric template therefrom. Clearview generated biometric information (a "Faceprint") enabling the identification of Plaintiff in direct violation of the laws identified in this Complaint, including the BIPA. Clearview then sold, marketed, advertised, or otherwise made commercial use of access to its database containing Plaintiff's photograph and Faceprint to third-party entities throughout the United States generally, and in the states of New York and Illinois particularly, for a commercial monetary gain in an amount to be determined at trial.

13. Plaintiff never consented, agreed, or gave permission – written or otherwise – to Clearview to collect, capture, purchase, receive through trade, obtain, sell, lease, trade, disclose, redisclose, disseminate, or otherwise profit from or use his photograph, likeness, and biometric information and identifiers. Likewise, Clearview never informed Plaintiff by written notice or otherwise that Plaintiff could prevent Clearview from collecting, capturing, purchasing, receiving through trade, obtaining, selling, leasing, trading, disclosing, redisclosing, disseminating, or otherwise profiting from or using his photograph, likeness, and biometric information and identifiers. Similarly, Plaintiff was never provided with an opportunity to prohibit or prevent Clearview from collecting, capturing, purchasing, receiving through trade, obtaining, selling, leasing, trading, disclosing, redisclosing, disseminating, or otherwise profiting from or using his photograph, likeness, and biometric information and identifiers.

14. As a result of Clearview's unauthorized collecting, capturing, purchasing, receiving through trade, obtaining, selling, leasing, trading, disclosing, redisclosing, disseminating, or otherwise profiting from or using Plaintiff's photograph, likeness, and biometric information and identifiers, Plaintiff was deprived of his control over that valuable and sensitive information. By

depriving him of his control over this valuable information, Clearview misappropriated the value of his photograph, likeness, and biometric information and identifiers. Consequently, Clearview has unlawfully profited therefrom. Plaintiff has further suffered damages in the diminution in value of his sensitive biometric information and identifiers – information which is now at higher risk of privacy violations.

Defendant Clearview AI, Inc.

15. Defendant Clearview AI, Inc., is a private, for-profit Delaware corporation, with its principal place of business located in New York, New York. Clearview markets, advertises, sells, and otherwise makes commercial use of its product throughout the United States, including in New York and Illinois, among others. Based on information and belief, Clearview illicitly scraped the images of faces of billions of consumers from websites and platforms that are owned and operated by Illinois-based companies. In other words, Defendants are unlawfully using biometric information and identifiers in Illinois. Defendants' conduct in Illinois is specifically harming residents from Illinois, New York, and throughout the United States in multiple ways, including: (a) Defendants' illicit scraping of images of their faces from servers in Illinois, among others; and (b) Defendants' unlawful selling, using, or otherwise disclosing of their biometric information, identifiers, and likeness to business entities in Illinois, such as the Chicago Police Department, who are then also violating some of the laws at issue in this Complaint.

16. Defendant Clearview is a "private entity" within the meaning of the BIPA, which defines "private entity" as "any individual, partnership, corporation, [etc.] . . . however organized." 740 ILCS 14/10.

Defendant Hoan Ton-That

17. Defendant Hoan Ton-That is a founder and the Chief Executive Officer ("CEO") of Clearview. Defendant Ton-That is a resident and citizen of New York. He is a "private entity"

within the meaning of the BIPA, which defines "private entity" as "any individual, partnership, corporation, [etc.] . . . however organized." *Id.*

18. As a founder and the CEO of Clearview, Defendant Ton-That knew of, participated in, consented to, approved, authorized, and directed the wrongful acts alleged in this Complaint. Based on information and belief, Defendant Ton-That conspired with Clearview and its other owners/shareholders, officers, and/or directors, including, without limitation, Defendant Schwartz, to carry out the illegal scheme alleged in this Complaint.

Defendant Richard Schwartz

19. Defendant Richard Schwartz is a founder and, based on information and belief, an officer, director, and/or principal of Clearview. Defendant Schwartz is a resident and citizen of New York. He is a "private entity" within the meaning of the BIPA, which defines "private entity" as "any individual, partnership, corporation, [etc.] . . . however organized." *Id.*

20. As a founder and officer, director, and/or principal of Clearview, Defendant Schwartz knew of, participated in, consented to, approved, authorized, and directed the wrongful acts alleged in this Complaint. Based on information and belief, Defendant Schwartz conspired with Clearview and its other owners/shareholders, officers, and/or directors, including, without limitation, Defendant Ton-That, to carry out the illegal scheme alleged in this Complaint.

Defendants Conspired Amongst Themselves and With Others to Carry Out the Unlawful Scheme

21. Defendants conspired amongst themselves and, based on information and belief, with the other owners, directors, officers, and/or shareholders of Clearview (the "Co-Conspirators") to carry out the unlawful scheme, including the intentional torts. Defendants and the Co-Conspirators knew and/or had reason to know about Clearview's primary business function, which was to scrape the internet for images of faces, use facial recognition technology

to generate biometric information and identifiers, and sell access to the same to third-party entities and agencies, without the consent of the consumers whose photographs, likenesses, and biometric information and identifiers were being used. Defendants and the Co-Conspirators agreed to this business plan – a plan, which, when carried out, violated several laws, including, *inter alia*, the BIPA. Defendants and the Co-Conspirators intended to profit from the primary, albeit unlawful, business plan of Clearview.

22. Defendants each had knowledge of the unlawful business purpose, consented to and authorized the fulfillment of the unlawful business purpose, and directed and otherwise carried out the unlawful business purpose of the unauthorized collecting, capturing, purchasing, receiving through trade, obtaining, selling, leasing, trading, disclosing, redisclosing, disseminating, or otherwise profiting from and/or using Plaintiff's and the Class's photographs, likenesses, and biometric information and identifiers without their consent.

23. Each of the Co-Conspirators are responsible as joint tortfeasors for all damages ensuing from the wrongful conduct carried out by Defendants. Each member of the conspiracy is liable for all acts done by others pursuant to the conspiracy and for all damages caused thereby.

24. The true names and capacities of defendants sued herein as Does 1 through 10, inclusive, are presently not known to Plaintiff, who therefore sues these Defendants by such fictitious names. Plaintiff will seek to amend this Complaint and include these Doe Defendants' true names and capacities when they are ascertained. Each of the fictitiously named Doe Defendants is responsible in some manner for the conduct alleged herein and for the injuries suffered by Plaintiff and the Class.

FACTUAL ALLEGATIONS

A. Biometrics and Privacy

25. "Biometrics" refers to technologies used to identify an individual based on unique physical characteristics, *e.g.*, "face geometry." Throughout the last several years, companies have developed facial recognition technology, which works by scanning an image for human faces, extracting facial feature data from the image, generating a "faceprint" through the use of facial-recognition algorithms, and then comparing the resultant faceprint to other faceprints stored in a database. If a match is found, a person may be identified, including sensitive and confidential information about that person.

26. This technology has raised serious privacy concerns about its massive scope and surreptitiousness. For example, in 2011, Google's Chairman at the time said it was a technology the company held back on because it could be used "in a very bad way." Senator Markey recognized that widespread use of the technology "could facilitate dangerous behavior and could effectively destroy individuals' ability to go about their daily lives anonymously."[4]

27. The Illinois Legislature has acknowledged that the "full ramifications of biometric technology are not fully known." 740 ILCS 14/5(f). It is known, however, that the "public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." 740 ILCS 14/5(g).

28. "Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5(c). "For example, social security numbers, when compromised, can be changed." *Id.* "Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse [and] is at heightened risk

[4] Markey Letter, *supra* n.1.

for identity theft[.]" *Id.* Recognizing this problem, the Federal Trade Commission urged companies using facial recognition technology to ask for consent ***before*** scanning and extracting biometric data from photographs.[5] This prevailing view has been adopted by the BIPA, which requires notice to and consent from the person who's biometric identifier or information is being used. Unfortunately, Defendants could care less about the prevailing view or the BIPA and failed to obtain user consent before launching Clearview's wide-spread facial recognition program and continue to violate millions of individual's legal privacy rights.

B. Illinois's Biometric Information Privacy Act ("BIPA")

36. The BIPA was enacted in 2008. Under the BIPA, companies may not:

> [C]ollect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier[] unless it first:
>
> (1) informs the subject . . . in writing that a biometric identifier . . . is being collected or stored;
>
> (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier . . . is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier.

740 ILCS 14/15(b).

37. The statute defines "biometric identifier" to include "retina or iris scan, fingerprint, voiceprint, or scan of hand or ***face geometry***." 740 ILCS 14/10 [emphasis added]. "'Biometric Information' means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." *Id.*

38. The BIPA also regulates how companies acting within Illinois must handle biometric identifiers and information. *See* 740 ILCS 14/15(c)-(d). For example, the law prohibits selling, leasing, trading, or otherwise profiting from a person's biometric data. 704 ILCS 14/15(c).

---

[5] *See Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, FED. TRADE COMM'N (Oct. 2012), https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

The BIPA also requires companies like Clearview to develop a publicly available written policy "establishing a retention schedule and guidelines for permanently destroying biometric" data. 740 ILCS 14/15(a).

C. Clearview Knowingly and Intentionally Violated the BIPA

39. As explained below, Defendants unlawfully collected, captured, purchased, received through trade, obtained, sold, leased, traded, disclosed, redisclosed, disseminated, and/or otherwise profited from or used Plaintiff's and the Class's photographs and biometric information and identifiers in violation of the BIPA. Clearview has been described by the media as the "secretive company that might end privacy as we know it."[6]

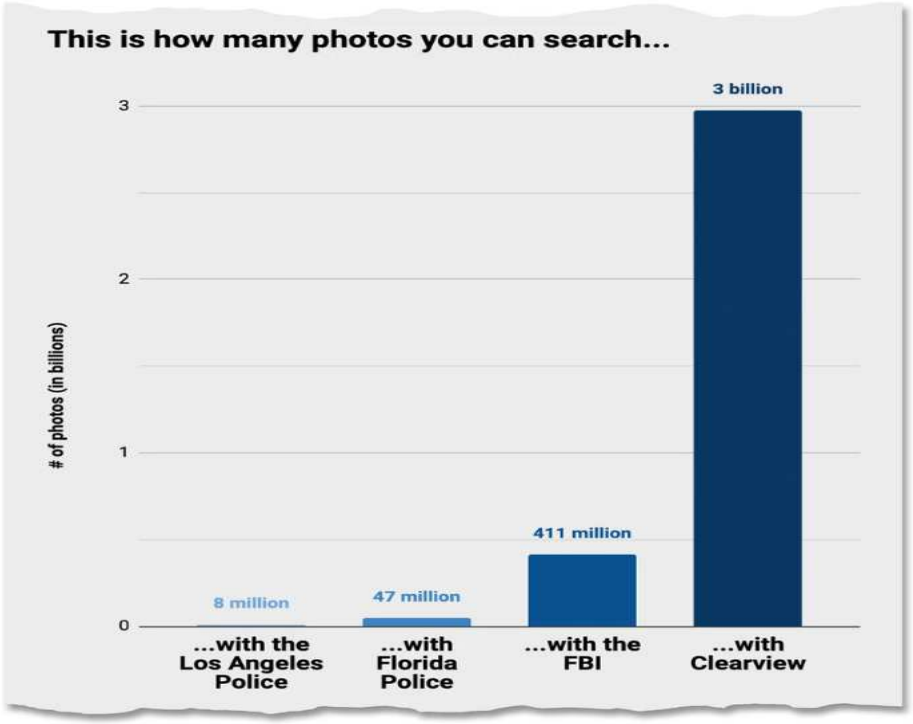
40. Clearview uses a software application to illicitly and secretly scrape billions of images from websites, such as Twitter, Facebook, Venmo, Google, Instagram, and YouTube, in violation of many of the websites' policies. Indeed, companies, such as Facebook and Twitter, have sent Clearview cease and desist letters. Based on information and belief, Clearview's web scraping software accesses data, which includes the photographs and likenesses of Plaintiff and Class members, is stored on servers throughout the United States.

41. Clearview's software application then applies facial recognition software to the illicitly scraped images, whereby the company uses artificial intelligence algorithms to scan the facial geometry of faces in the images. The algorithm calculates an individual face's unique physical characteristics, which result in a biometric template that is separate and distinct from the image from which it was created. Clearview describes the technology as a "state-of-the-art neural net" to convert all images into mathematical formulas, or "vectors," based on facial geometry –

[6] *See*, *e.g.*, Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020; updated Feb. 10, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

like how far apart a person's eyes are. This process generates biometric information enabling the identification of the individuals in the images (herein referred to as individuals' "Faceprint") in direct violation of the BIPA. Defendants engage in this process without notifying any of the individuals whose images Clearview has captured, converted into a Faceprint, stored, and shared for a profit. Defendants certainly have not obtained these individuals' consent – written or otherwise.

42. Once Defendants generate the biometric information for millions of people, Clearview sells access to the database to law enforcement agencies and private companies. Instead of having limited photo arrays, agencies and private companies are now able to use Clearview's database of three billion photos:



A chart from marketing materials that Clearview provided to law enforcement.
Clearview

43. These agencies and companies have instantaneous access to the biometric information of billions of people allowing them to peep into almost every aspect of their digital lives, including who they associate with, where they live, etc.

44. Defendants also have real-time access to monitor which individuals law enforcement agencies are searching for. For example, an investigative journalist from *The New York Times*, who was doing a story on Clearview, had a law enforcement agency upload images of his face and run it through Clearview's application. Soon thereafter, the agency received calls from Clearview asking if it was talking to the media – a clear sign Clearview has the ability and appetite to monitor whom law enforcement is searching for.

45. In addition, based on information and belief, the computer code underlying Clearview's software application includes programmable language to enable it to pair with augmented reality glasses. This tool potentially enables any user wearing the glasses to identify in real-time every person they see as they walk down the street, potentially revealing not just their names, but where they live, what they like to do, and who they know and associate with.

46. Moreover, it has been shown that Clearview cannot adequately safeguard the biometric information and identifiers of Plaintiff and the Class. On February 26, 2020, it was publicly reported that there was a data breach of Clearview's data storage servers, which compromised the privacy and security of every person whose image Clearview had scraped and used to generate biometric identifiers.

47. Defendants' violations of the BIPA continue to this day. Clearview continues to scrape and sell access to the photographs and biometric information that Class members upload to social media sites. Neither Plaintiff nor Class members have any ability to enjoin Defendants from

their unlawful activity. These ongoing violations of the BIPA evidence a continuing risk of substantial harm that is concrete, particularized, and imminent.

48. The result of Clearview's technology is a profit machine for a single company that relies on the secret use of individual's biometric information. This is a radical evasion and erosion of privacy. Defendants are laying the groundwork for a dystopian future and violating, *inter alia*, the BIPA in the process.

CLASS ACTION ALLEGATIONS

49. Plaintiff realleges and incorporates herein by reference each allegation in the preceding and subsequent paragraphs.

50. Plaintiff brings this action individually and on behalf of a class of similarly situated individuals pursuant to Rule 23 of the Federal Rules of Civil Procedure.

51. As used herein, the term "Illinois Biometric Information" means "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual[,]" as defined in the BIPA, 740 ILCS 14/10.

52. Plaintiff seeks to represent the following classes of persons:

(a) **Sub-Class One (the "BIPA Class") (740 ILCS 14/1, *et seq.*):**

All persons in the United States who had their Illinois Biometric Information collected, captured, purchased, received, obtained, sold, leased, traded, disclosed, redisclosed, disseminated, and/or otherwise profited from and/or used by any of the Defendants without their consent.

(b) **Sub-Class Two (the "Unjust Enrichment Class"):**

All persons in the United States who had their Illinois Biometric Information collected, captured, purchased, received, obtained, sold, leased, traded, disclosed, redisclosed, disseminated, and/or otherwise profited from and/or used by any of the Defendants without their consent, from which any of the Defendants were unjustly enriched.

53. Sub-Class One and Sub-Class Two are collectively referred to herein as the "Class."

54. Excluded from the Class are Defendants Ton-That, Schwartz, and Clearview, including its officers and directors, families, owners, and legal representatives, heirs, successors, or assigns, and any entity in which Clearview have a controlling interest, and any judge or court staff assigned to this case and their immediate families.

55. Plaintiff reserves the right to amend or modify the Class definition in connection with his motion for class certification, as a result of discovery, at trial, or as otherwise allowed by law.

56. Plaintiff brings this action individually and on behalf of all others similarly situated because there is a well-defined community of interest in the litigation and the proposed Class is easily ascertainable.

Numerosity

57. The potential members of the Class, and each of the sub-classes independently, are so numerous that joinder of all the members is impracticable. While the precise number of members of the Class, or each of the sub-classes, has not been determined, Plaintiff is informed and believes the Class, and each of the sub-classes, include at least thousands (and potentially even millions) of individuals.

58. Based on information and belief, Clearview's records evidence the number and location of the Class, and each of the sub-classes, respectively.

Commonality and Predominance

59. There are questions of law and fact common to the Class that predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

(a) whether Clearview collected, captured, received, or otherwise obtained Plaintiff's and the BIPA Class's Illinois Biometric Information;

(b) whether Clearview has sold, leased, traded, or otherwise profited from Plaintiff's and the BIPA Class's Illinois Biometric Information;

(c) whether Clearview disclosed, redisclosed, or otherwise disseminated Plaintiff's and the BIPA Class's Illinois Biometric Information;

(d) whether Clearview properly informed Plaintiff and the BIPA Class that it collected, captured, purchased, received, obtained, sold, leased, traded, disclosed, redisclosed, disseminated, and/or otherwise profited from and/or used their Illinois Biometric Information;

(e) whether Clearview obtained a written release (as defined in 740 ILCS 14/10) from Plaintiff and the BIPA Class to collect, capture, or otherwise obtain their biometric identifiers;

(f) whether Clearview made publicly available to Plaintiff and the BIPA Class a written policy establishing a retention schedule and guidelines for permanently destroying Illinois Biometric Information in compliance with the BIPA;

(g) whether Clearview's violations of the BIPA were committed intentionally, recklessly, or negligently;

(h) whether Clearview was unjustly enriched by the misappropriation of Plaintiff's and the Unjust Enrichment Class's Illinois Biometric Information;

(i) whether Defendants conspired for the purpose of accomplishing some concerted action for either an unlawful purpose or lawful purpose by unlawful means; and

(j) whether Plaintiff and the Class have been harmed and the proper measure of relief.

Typicality

60. The claims of Plaintiff are typical of the claims of the Class. Plaintiff and all members of the Class sustained injuries and damages arising out of, and caused by, Defendants' common course of conduct in violation of laws, regulations that have the force and effect of law, and statutes as alleged herein.

Adequacy of Representation

61. Plaintiff will fairly and adequately represent and protect the interests of the Class. Counsel who represents Plaintiff are competent and experienced in litigating large consumer class actions.

Superiority of Class Action

62. A class action is superior to other available means for the fair and efficient adjudication of this controversy. Individual joinder of Class members is not practicable, and questions of law and fact common to the Class predominate over any questions affecting only individual Class members. Each member of the Class has been damaged and is entitled to recovery because of Clearview's uniform unlawful policy and/or practices described herein. There are no individualized factual or legal issues for the Court to resolve that would prevent this case from proceeding as a class action. Class action treatment will allow those similarly situated persons to litigate their claims in the manner that is most efficient and economical for the parties and the judicial system. Plaintiff is unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

COUNT I
Violation of the BIPA
740 ILCS 14/1, *et seq*.
(On Behalf of Plaintiff and the BIPA Class Against All Defendants)

63. Plaintiff hereby realleges and incorporates by reference the allegations contained in the paragraphs above as if fully set forth herein.

64. Defendants violated the following sections of the BIPA:

(a) 740 ILCS 14/15(a);

(b) 740 ILCS 14/15(b);

(c) 740 ILCS 14/15(c); and

(d) 740 ILCS 14/15(d).

65. Section 15(a) of the BIPA requires that:

> [Any] private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.

740 ILCS 14/15(a).

66. Section 15(b) of the BIPA makes it unlawful for any private entity to, among other things:

> [C]ollect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:
>
> (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or biometric information.

740 ILCS 14/15(b).

67. Section 15(c) of the BIPA makes it unlawful for any private entity to, among other things, "sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information." 740 ILCS 14/15(c).

68. Section 15(d) of the BIPA makes it unlawful for any private entity to, among other things:

> [D]isclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:
>
> (1) the subject of the biometric identifier or biometric information . . . consents to the disclosure or redisclosure;
>
> (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information . . .;
>
> (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or
>
> (4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

740 ILCS 14/15(d).

69. Defendants violated Sections 15(a)-(d) of the BIPA. Preliminarily, Clearview is a Delaware corporation and thus qualifies as a "private entity" under the BIPA. *See* 740 ILCS 14/10. Defendants Ton-That and Schwartz are "individuals" and, thus, are each a "private entity" under the BIPA. *Id.*

70. Plaintiff's and the Class's Faceprints are "biometric identifiers" and "biometric information" pursuant to 740 ILCS 14/10.

71. During the relevant period, Defendants did not make available to the public a written policy establishing a retention schedule and guidelines for permanently destroying Plaintiff's and the BIPA Class's biometric identifiers and biometric information, as specified by the BIPA. *See* 740 ILCS 14/15(a). Thus, Defendants violated Section 15(a) of the BIPA.

72. Defendants systematically and automatically collected, captured, purchased, received, and/or otherwise obtained Plaintiff's and the BIPA Class's biometric identifiers and/or

biometric information without first obtaining the specific written release required by 740 ILCS 14/15(b)(3). Likewise, Defendants did not properly inform Plaintiff or the BIPA Class in writing that their biometric identifiers and/or biometric information were being collected, captured, purchased, received, and/or otherwise obtained, nor did it inform them in writing of the specific purpose and length of term for which their biometric identifiers and/or biometric information were being collected, captured, purchased, received, and/or otherwise obtained, as required by 740 ILCS 14/15(b)(1)-(2). Thus, Defendants violated Section 15(b) of the BIPA.

73. Defendants knowingly sold, leased, traded, and/or otherwise profited from Plaintiff's and the BIPA Class's biometric identifiers and/or biometric information. Thus, Defendants violated Section 15(c) of the BIPA.

74. Defendants also disclosed, redisclosed, and/or otherwise disseminated Plaintiff's and the BIPA Class's biometric identifiers and/or biometric information without obtaining the consent from Plaintiff and the BIPA Class and/or their authorized representatives. The disclosure, redisclosure, and/or dissemination by Defendants of Plaintiff's and the BIPA Class's biometric identifiers and/or biometric information was not to complete a financial transaction requested or authorized by Plaintiff or members of the BIPA Class, nor was the disclosure and/or redisclosure required by state or federal law, municipal ordinance, or required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction. Thus, Defendants violated Section 15(d) of the BIPA.

75. Defendants Ton-That and Schwartz conspired with Clearview and the Co-Conspirators to carry out the unlawful scheme set forth above. They each had direct knowledge of the scheme and consented, participated, directed, and otherwise assisted in carrying out the

unlawful scheme. Based on information and belief, Defendants are continuing to direct and carry out the unlawful scheme.

76. Plaintiff and the BIPA Class have been directly harmed by Defendants' violations of Sections 14/15(a)-(d) of the BIPA. They have been deprived of their control over their valuable information and otherwise suffered monetary and non-monetary losses. By depriving Plaintiff and the BIPA Class of control over their valuable information, Defendants misappropriated the value of their biometric identifiers and/or biometric information. Based on information and belief, Defendants have profited from their unlawful conduct.

77. On behalf of Plaintiff and the BIPA Class, Plaintiff seeks: (a) injunctive and equitable relief, as necessary, to protect the interests of Plaintiff and the BIPA Class by requiring Defendants to comply with the BIPA's requirements; (b) statutory damages of $5,000 per intentional or reckless violation of the BIPA, pursuant to 740 ILCS 14/20(2), and statutory damages of $1,000 per negligent violation of the BIPA, pursuant to 740 ILCS 14/20(1); and (c) reasonable attorneys' fees, costs, and other litigation expenses, pursuant to 740 ILCS 14/20(3).

COUNT II
Unjust Enrichment/Restitution
(On Behalf of Plaintiff and the Unjust Enrichment Class
Against Defendant Clearview)

78. Plaintiff hereby realleges and incorporates by reference the allegations contained in the paragraphs above as if fully set forth herein.

79. Clearview was unjustly enriched by its unlawful misappropriation of Plaintiff's and the Unjust Enrichment Class's Illinois Biometric Information. Through its unlawful conduct, Clearview received and retained a benefit it otherwise would not have achieved. By depriving Plaintiff and the Unjust Enrichment Class of control over their valuable Illinois Biometric Information, Clearview took control of and misappropriated the value of their Illinois Biometric

Information. Clearview's conduct also exposed Plaintiff and the Unjust Enrichment Class to a heightened risk of an invasion of their privacy.

80. There is not another adequate remedy at law. It would be unjust and unfair for Clearview to retain any of the benefits obtained from its unlawful misappropriation of Plaintiff's and the Unjust Enrichment Class's Illinois Biometric Information. Clearview should be ordered to disgorge the proceeds that it unjustly received from the misappropriation of Plaintiff's and the Unjust Enrichment Class's Illinois Biometric Information.

COUNT III
Request for Relief Under the Declaratory Judgment Act
28 U.S.C. §§2201, *et seq.*
(On Behalf of Plaintiff and the Class Against Defendant Clearview)

81. Plaintiff hereby realleges and incorporates by reference the allegations contained in the paragraphs above as if fully set forth herein.

82. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and that violate the terms of the statutes described in this Complaint.

83. An actual controversy has arisen in the wake of Defendants' unlawful collection, disclosure, sale, and misuse of Plaintiff's and the Class's photographs and biometric identifiers and information without their consent, as alleged herein, in violation of Defendants' common law and statutory duties.

84. Plaintiff continues to suffer injury and damages, as described herein, as Defendants continue to collect, disclose, sell, and misuse Plaintiff's and Class members' photographs and biometric identifiers and information.

85. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

(a) Defendants continue to owe a legal duty to not collect, disclose, sell, and otherwise misuse Plaintiff's and Class members' photographs and biometric identifiers and information under, *inter alia*, the common law and the BIPA, 740 ILCS 14/1, *et seq*.

(b) Defendants continue to breach their legal duties to Plaintiff and Class members by continuing to collect, disclose, sell, and otherwise misuse Plaintiff's and Class members' photographs and biometric identifiers and information; and

(c) Defendants' ongoing breaches of their legal duty continue to cause Plaintiff and Class members harm.

86. The Court should also issue corresponding injunctive relief, including, but not limited to, enjoining Defendants from engaging in the unlawful conduct alleged in this claim and requiring Defendants to delete all photographs and biometric identifiers and information of Plaintiff and Class members and cease further collecting of such information or engaging in any activities that would result in the disclosure, sale, or misuse of Plaintiff's and Class members' photographs and biometric identifiers and information. If an injunction is not issued, Plaintiff will suffer irreparable injury and lack an adequate legal remedy in the event the statutory or common law does not prohibit, among other things, the collection, disclosure, sale, and misuse of photographs and biometric identifiers and information. Illinois specifically constrains the collection, disclosure, and sale of biometric information and recognizes a person's right to maintain such personal information as private. In light of Defendants' persuasive flaunting of such rights, including the continued collection, disclosure, sale, and misuse of Plaintiff's and Class members' photographs and biometric identifiers and information, the risk of continued violations

of Illinois law and the common law is real, immediate, and substantial. Plaintiff does not have an adequate remedy at law because many of the resulting injuries are reoccurring and Plaintiff will be forced to bring multiple lawsuits to rectify the same conduct.

87. The hardship to Plaintiff and the Class if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. On the other hand, the cost to Defendants of complying with an injunction by complying with Illinois law and the common law by ceasing to engage in the misconduct alleged herein is relatively minimal, and Defendants have a pre-existing legal obligation to avoid invading the privacy rights of consumers.

88. Issuance of the requested injunction will serve the public interest by preventing ongoing collection, disclosure, sale, and misuse of photographs and biometric identifiers and information without consent, thus eliminating the injuries that would result to Plaintiff and the Class, and the hundreds of millions of Americans who upload photographs to social media sites.

PRAYER FOR RELIEF

Wherefore, Plaintiff, individually and on behalf of the Class, respectfully requests that this Court enter an Order:

A. Certifying this action as a class action on behalf of the sub-classes defined above, appointing Plaintiff as the representative of the Class, and appointing his counsel as Class Counsel;

B. Declaring that Defendants' actions, as set forth above, violate the BIPA, 740 ILCS 14/1, *et seq*.;

C. Awarding compensatory, non-compensatory, statutory, exemplary, and punitive damages;

D. Awarding statutory damages of $5,000 per intentional or reckless violation of the BIPA, pursuant to 740 ILCS 14/20(2), and statutory damages of $1,000 per negligent violation of the BIPA, pursuant to 740 ILCS 14/20(1);

E. Awarding restitution of all monies, expenses, and costs due to Plaintiff and the Class;

F. Awarding Plaintiff and the Class their reasonable attorneys' fees, costs, and litigation expenses;

G. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable;

H. Awarding injunctive and other equitable relief, as necessary, to protect the interests of the Class, including, among other things, an order requiring Defendants to comply with the BIPA and enjoining Defendants from engaging in the unlawful conduct alleged herein; and

I. Awarding such other and further relief as equity and justice may require.

JURY DEMAND

Plaintiff, individually and on behalf of the Class, hereby demands trial by jury on all issues so triable.

Dated: April 15, 2020

SCOTT+SCOTT ATTORNEYS AT LAW LLP

/s/ Joseph P. Guglielmo

Joseph P. Guglielmo
Carey Alexander
The Helmsley Building
230 Park Avenue, 17th Floor
New York, NY 10169
Telephone: 212-223-6444
Facsimile: 212-223-6334
jguglielmo@scott-scott.com
calexander@scott-scott.com

Erin Green Comite
Margaret B. Ferron
SCOTT+SCOTT ATTORNEYS AT LAW LLP
156 South Main Street
P.O. Box 192
Colchester, CT 06415
Telephone: 860-537-5537

Facsimile: 860-537-4432
ecomite@scott-scott.com
mferron@scott-scott.com

Amber L. Eck
Alreen Haeggquist
Aaron M. Olsen
Ian Pike
HAEGGQUIST & ECK, LLP
225 Broadway, Suite 2050
San Diego, CA 92101
Telephone: 619-342-8000
Facsimile: 619-342-7878
ambere@haelaw.com
alreenh@haelaw.com
aarono@haelaw.com
ianp@haelaw.com

Attorneys for Plaintiff and the Proposed Class