Ronald A. Marron (SBN 175650)
Alexis M. Wood (SBN 270200)
Kas L. Gallucci (SBN 288709)
LAW OFFICES OF RONALD A.
MARRON, APLC
651 Arroyo Drive
San Diego, California 92103
Tel: 619.696.9006
Fax: 619.564.6665

J. Dominick Larry (*pro hac vice* to be sought)
NICK LARRY LAW LLC
55 E Monroe St, Suite 3800
Chicago, Illinois 60603
Tel: 773.694.4690
Fax: 773.694.4691

Counsel for Plaintiff and the Putative Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA – SAN FRANCISCO DIVISION

LYNETTE WALTON, on behalf of herself, and all others similarly situated, Plaintiff, v. EVERALBUM, INC., d/b/a PARAVISION a Delaware Corporation, Defendant.	Case No.: CLASS ACTION **COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiff Lynette Walton brings this Class Action Complaint and Demand for Jury Trial ("Complaint") against Defendant Everalbum Inc., d/b/a Paravision, for violating the Illinois Biometric Information Privacy Act, 740 ILCS 14/1–99 ("BIPA"). Plaintiff alleges the following upon personal knowledge as to herself and her own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by her attorneys:

NATURE OF THE ACTION

1. Paravision is an artificial-intelligence software company that provides facial-recognition technology to law-enforcement agencies, militaries, defense contractors, and other private businesses.

2. Facial-recognition technology is complex. Modern facial-recognition applications typically make use of machine-learning technology, which uses artificial intelligence to train computer systems on complex tasks.

3. For machine learning to work in the facial-recognition context, it requires a large data set. That is, it needs photos. Lots of photos.

4. Every company that has developed its own facial-recognition software has faced a similar dilemma: where to get enough photos of faces—with sufficient variance in photo quality, lighting, and face shapes and features—to create a robust, functional system.

5. Paravision's solution was novel, but also highly deceptive and illegal.

6. To build its training database of faces, Paravision mined Everalbum (later rebranded as Ever). Everalbum was a website—and later, as Ever, an app—operated by Defendant, offering cloud photo storage. Unbeknownst to its users, however, the billions of photos they uploaded were fuel for Paravision's AI machine. While users may have thought they were merely ensuring the lasting

storage of "Weekend with Grandpa" photos,[1] they were instead unwittingly ushering in a corporate surveillance dystopia.

7. Illinois's legislature saw this problem coming. In 2008, it enacted the Biometric Information Privacy Act, 740 ILCS 14/1–99 ("BIPA"), which regulates the use of biometric data (including facial-recognition scans), prohibits its capture without consent, and outright prohibits companies from profiting off it.

8. Thus, Paravision's systematic and covert privacy intrusion is plainly unlawful in Illinois.

9. Plaintiff brings this Complaint seeking an order (i) declaring that Paravision's conduct violates BIPA, (ii) requiring that Paravision cease the unlawful activities described herein and destroy the biometric data it unlawfully collected, and (iii) awarding Plaintiff and the Class statutory damages of $5,000 per violation, plus their attorneys' fees and costs.

PARTIES

10. Plaintiff is a natural person and a citizen of the State of Illinois.

11. Paravision is a Delaware corporation, with its headquarters and principal place of business located at 1160 Gorgas Ave, San Francisco, California 94129. Paravision conducts business throughout this District and the State of California.

INTRADISTRICT ASSIGNMENT

12. Pursuant to Local Rule 3-2(c), this action is appropriate for assignment to the San Francisco Division because Paravision is headquartered in San Francisco County.

[1] Olivia Solon and Cyrus Farivar, *Millions of people uploaded photos to the Ever app. Then the company used them to develop facial recognition tools*, NBC News (May 9, 2019), https://www.nbcnews.com/tech/security/millions-people-uploaded-photos-ever-app-then-company-used-them-n1003371 (last visited on September 29, 2020).

JURISDICTION AND VENUE

13. This Court has jurisdiction over the subject-matter of this action pursuant to 28 U.S.C. § 1332(d) because Plaintiff is a citizen of a state different from Defendant, and because Plaintiff seeks more than $5,000,000 in damages.

14. This Court has personal jurisdiction over Paravision because it is headquartered in this District.

15. Venue is proper in this District under 28 U.S.C. § 1391(b) because Paravision resides in this District.

COMMON FACTUAL ALLEGATIONS

The Biometric Information Privacy Act

16. Illinois enacted BIPA in 2008 after a company called Pay By Touch, "the largest fingerprint scan system in Illinois," filed for bankruptcy, leaving "thousands of customers wondering what [would] become of their biometric and financial data." 95th Ill. Gen. Assem., House Proceedings, May 30, 2008, at 249 (statement of Representative Ryg). Citing the risks created by the bankruptcy court's sale of Pay By Touch's database, Rep. Ryg identified the "very serious need of protections for the citizens of Illinois when it comes to biometric information." *Id.*

17. The legislative findings accompanying BIPA recognize the unique and persistent nature of biometric identifiers, that the "overwhelming majority of members of the public are weary of the use of biometrics," and that "[t]he full ramifications of biometric technology are not fully known." 740 ILCS 14/5(d), (f).

18. Citing these concerns, the legislature determined that the "public welfare, security, and safety [would] be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." 740 ILCS 14/5(g). Accordingly, it enacted a comprehensive regime to ensure the informed consent of subjects to the collection, use, disclosure, and retention of biometric data.

19. BIPA regulates two types of biometric data. First, any "biometric identifier," which means "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry," and specifically excludes a lengthy list of identifiers outside that scope. Second, any "biometric information," which "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." 740 ILCS 14/10. Biometric information "does not include information derived from items or procedures excluded under the definition of biometric identifiers." *Id.*

20. BIPA regulates the entire lifecycle of biometric data, from capture and collection to use and disclosure.

21. As to the origination of biometric data, BIPA provides that "[n]o private entity may collect, 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 or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject or the subject's legally authorized representative 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 or the subject's legally authorized representative."

22. BIPA likewise restricts the disclosure of biometric data, providing that "[n]o private entity in possession of a biometric identifier or biometric information may disclose, 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 or the subject's legally authorized representative 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 biometric information or the subject's legally

authorized representative; (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).

23. When it comes to use of biometric data, BIPA creates even stricter proscriptions. Reflecting an intent to preclude the formation of a market for biometric data, BIPA provides without exception that "[n]o private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information." 740 ILCS 14/15/(c).

24. To facilitate the informed notice and consent provisions described above, BIPA also requires that any private entity in possession of biometric identifiers or information must publish a written policy "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).

25. Finally, given the persistent nature of biometric data and the increased risks that accompany their misuse, BIPA requires that any entity possessing biometric identifiers or information "(1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and (2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information." 740 ILCS 14/15(e).

26. To remedy the serious but often intangible harms that accompany invasions of biometric privacy rights, BIPA also includes a private right of action

authorizing "[a]ny person aggrieved by a violation of" the statute to sue and recover for each violation liquidated damages of $1,000, or $5,000 in the event of an intentional or reckless violation, plus attorneys' fees, costs, and appropriate injunctive relief. 740 ILCS 14/20.

Paravision's Wanton Disregard for People's Privacy

27. Illinois's vanguard biometric privacy law has made headlines for several years, largely as a result of high-profile lawsuits, including several in Paravision's backyard. Nonetheless, Paravision disregarded BIPA in its entirety.

28. Paravision's facial-recognition systems facilitate a number of end-uses, including point-of-sale processing, facility access controls, video security, identity verification, and more.

29. To accomplish any of those goals, however, Paravision's software must be able to identify specific individuals in a variety of settings, poses, outfits, and lighting scenarios. Training the software to function with high accuracy in the face of these obstacles and across ages, races, and genders requires an enormous amount of photo data from which to draw.

30. For years, the photographic datasets available for facial-recognition training were deficient. Generally lacking in diversity, the systems trained on these datasets often lacked accuracy when analyzing faces of women or people of color.

31. In recent years, as surveillance technology and high-definition camera systems have proliferated, facial-recognition developers have sought new sources of training data for their systems.

32. Photo-sharing and -storage apps and websites offered one solution. With a more diverse user base, these services did the hard work for the developers, effectively deputizing millions of amateur photographers the world over to assemble a sufficiently representative dataset.

33. Unlike its competitors, who used datasets provided by external photo-sharing and -storage services, Paravision used its own, in-house solution, Everalbum, later known as the Ever app.

34. With billions of photos from millions of users, Everalbum offered a comprehensive and exclusive training field for developing its own facial recognition tools that could be sold to law enforcement, intelligence, and various private industries.

35. Paravision took advantage of the opportunity offered by the Everalbum user data. Paravision fed the billions of photos uploaded to Everalbum into its machine-learning system, scanned and captured the geometry of any faces featured in those photos (known as a faceprint), and then used those faceprints to train its enterprise facial-recognition offerings.

36. Those enterprise facial-recognition offerings now form the entirety of Paravision's business, with the company having decided to shutter the (now unnecessary) Ever app in August 2020.

37. The problem with Paravision's solution is that its customers were completely unaware. Everalbum (and later Ever app) and Ever AI were two completely differentiated brands, and users of Everalbum/Ever would never have any reason to know that their photos were being used to build an artificially intelligent surveillance system.

38. Paravision never meaningfully informed Everalbum/Ever app users that their photos were being exploited, and only added a throwaway disclosure to its privacy policy after NBC News reporters contacted the company in 2019 in advance of publishing an exposé detailing the origins of Ever AI's facial-recognition systems.[2]

[2] Solon and Farivar, *supra* note 1.

39. Despite BIPA’s clear edict, Paravision never provided a publicly available biometric-data retention schedule, nor does it obtain customers’ informed, written consent prior to the collection, use, and disclosure of their biometric identifiers.

40. Worse still, Paravision then profits from its users’ faceprints, despite BIPA’s unambiguous prohibition on such profiteering.

FACTUAL ALLEGATIONS SPECIFIC TO PLAINTIFF

41. Plaintiff has used Paravision’s Everalbum service from approximately 2017 until recently.

42. Since Paravision implemented its facial-recognition system, Paravision has captured Plaintiff’s faceprint repeatedly, and has used those faceprints and her photos to train its enterprise facial recognition products.

43. By using Plaintiff’s faceprint to train its enterprise facial-recognition products, Paravision profited from Plaintiff’s biometric identifiers.

44. Paravision does not provide a publicly available retention schedule specifying the period for which it would retain Plaintiff’s faceprints.

45. Paravision has never informed Plaintiff of the purpose for which it was capturing or collecting her faceprint or the duration for which it would retain it, nor did Paravision receive a written release from Plaintiff authorizing the collection.

46. Because she was never informed of the collection of her faceprint, Plaintiff did not consent to the capture or collection of her faceprint.

CLASS ALLEGATIONS

47. Plaintiff brings this action pursuant to Fed. R. Civ. P. 23(b)(3) on behalf of herself and the following class (collectively, the “Class”):

> All individuals who had their faceprints collected, captured, received, or otherwise obtained by Paravision while residing in Illinois.

The following people are excluded from the Class: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendant, Defendant' subsidiaries, parents, successors, predecessors, and any entity in which the Defendant or its parents have a controlling interest and their current or former employees, officers, and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

48. **Numerosity**: The exact number of Class members is unknown to Plaintiff at this time, but it is clear that individual joinder is impracticable. Defendant has collected, captured, received, or otherwise obtained biometric identifiers or biometric information from hundreds of thousands, if not millions, of individuals within the Class definition. Ultimately, members of the Class will be identified through Defendant's records.

49. **Commonality and Predominance**: Questions of law and fact common to the claims of Plaintiff and the Class predominate over any questions that may affect individual members. Those common questions include:

a. Whether Defendant collected or captured the Class members' biometric identifiers;

b. Whether Defendant maintained a publicly available retention schedule for biometric identifiers;

c. Whether Defendant informed the Class members that it would collect or capture Class members' biometric identifiers;

d. Whether Defendant informed the Class members of the purpose for which they would collect their biometric identifiers, or the duration for which they would retain that data;

e. Whether Defendant obtained the written release required by BIPA to collect or capture, use, and store the Class members' biometric identifiers or information; and

f. Whether Defendant profited from the Class members' biometric identifiers.

50. **Typicality:** Plaintiff's claims are typical of the claims of the other members of the Class. Plaintiff and the Class suffered invasions of privacy as a result of Defendant's uniform wrongful conduct.

51. **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained competent counsel experienced in complex litigation and class actions under BIPA specifically. Plaintiff has no interests antagonistic to those of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the Class members and have the resources to do so.

52. **Superiority**: This class action is appropriate for certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy, and joinder of the Class members is otherwise impracticable. The damages suffered by the individual Class members are small relative to the burden and cost of individual litigation, and individual litigation is therefore infeasible. Even if Class members could sustain individual litigation, it would increase the delay and expense to all parties relative to a class action because of the complex factual issues raised by the Complaint. A class action presents fewer manageability difficulties and provides economies of scale and uniformity of decisions.

53. Plaintiff reserves the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

FIRST CAUSE OF ACTION
Violation of 740 ILCS 14/15(a)
On Behalf of Plaintiff and the Class

54. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

55. Paravision is a Delaware corporation and is therefore a "private entity" under 740 ILCS 14/10.

56. Plaintiff's and the Class's faceprints are scans of face geometry, and are therefore a "biometric identifier" under 740 ILCS 14/10.

57. Paravision failed to publicly provide the retention schedule or guidelines for permanently destroying their biometric identifiers as required by 740 ILCS 14/15(a).

58. On behalf of herself and the Class, and pursuant to 740 ILCS 14/20, Plaintiff seeks: (1) injunctive relief requiring Paravision to stop their unlawful practices and destroy the data unlawfully obtained; (2) liquidated damages of $5,000 per violation for Paravision's intentional and/or reckless violations of BIPA, or, in the event the Court finds those violations to be negligent, liquidated damages of $1,000 per violation; and (3) reasonable attorneys' fees and costs.

SECOND CAUSE OF ACTION
Violation of 740 ILCS 14/15(b)
On Behalf of Plaintiff and the Class

59. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

60. Paravision is a Delaware corporation and is therefore a "private entity" under 740 ILCS 14/10.

61. Plaintiff's and the Class's faceprints are scans of face geometry, and are therefore a "biometric identifier" under 740 ILCS 14/10.

62. Paravision systematically and automatically collected, used, and stored Plaintiff's and the Class's biometric identifiers without first obtaining the specific written release required by 740 ILCS 14/15(b)(3).

63. Paravision did not inform Plaintiff or the Class in writing that their biometric identifiers were being collected and stored, nor did it inform them in writing of the specific purpose and length for which their biometric identifiers would be collected, stored, and used, as required by 740 ILCS 14/15(b)(1)–(2).

64. On behalf of herself and the Class, and pursuant to 740 ILCS 14/20, Plaintiff seeks: (1) injunctive relief requiring Paravision to stop their unlawful practices and destroy the data unlawfully obtained; (2) liquidated damages of $5,000 per violation for Paravision's intentional and/or reckless violations of BIPA, or, in the event the Court finds those violations to be negligent, liquidated damages of $1,000 per violation; and (3) reasonable attorneys' fees and costs.

THIRD CAUSE OF ACTION
Violation of 740 ILCS 14/15(c)
On Behalf of Plaintiff and the Class

65. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

66. Paravision is a Delaware corporation and is therefore a "private entity" under 740 ILCS 14/10.

67. Plaintiff's and the Class's faceprints are scans of face geometry, and are therefore a "biometric identifier" under 740 ILCS 14/10.

68. By using Plaintiff's and the Class's faceprints to train its enterprise facial-recognition software, Paravision profited from Plaintiff's and the Class's biometric identifiers, in violation of 740 ILCS 14/15(c).

69. On behalf of herself and the Class, and pursuant to 740 ILCS 14/20, Plaintiff seeks: (1) injunctive relief requiring Paravision to stop their unlawful practices and destroy the data unlawfully obtained; (2) liquidated damages of

$5,000 per violation for Paravision's intentional and/or reckless violations of BIPA, or, in the event the Court finds those violations to be negligent, liquidated damages of $1,000 per violation; and (3) reasonable attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class, respectfully requests that this Court enter an order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff as representative of the Class, and appointing her lawyers as Class Counsel;

B. Declaring that Defendant's actions, as described above, violate 740 ILCS 14/15;

C. Awarding liquidated damages under 740 ILCS 14/20 of $5,000 per violation for Defendant's intentional and/or reckless violations of BIPA, or, alternatively, liquidated damages of $1,000 per violation if the Court finds that Defendant's violations were negligent;

D. Awarding injunctive and other equitable relief as necessary to protect the Class, including an order requiring Defendant to delete any such data that was unlawfully obtained;

E. Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys' fees;

F. Awarding Plaintiff and the Class pre- and post-judgment interest; and

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

JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

Date: October 2, 2020

LYNETTE WALTON, individually and on behalf of all others similarly situated,

s/ Ronald A. Marron

One of Plaintiff's Attorneys

Ronald A. Marron (SBN 175650)
Alexis M. Wood (SBN 270200)
Kas L. Gallucci (SBN 288709)
LAW OFFICES OF RONALD A. MARRON, APLC
651 Arroyo Drive
San Diego, California 92103
Tel: 619.696.9006
Fax: 619.564.6665

J. Dominick Larry (*pro hac vice* to be sought)
NICK LARRY LAW LLC
55 E Monroe St, Suite 3800
Chicago, Illinois 60603
Tel: 773.694.4690
Fax: 773.694.4691

Counsel for Plaintiff and the Putative Class