

CASE NO. 2022 CH 97

DATE: 1/5/2021

CASE TYPE: Class Action

PAGE COUNT: 19

CASE NOTE

12-Person Jury

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS COUNTY DEPARTMENT, CHANCERY DIVISION

DAVID ARENDT, *individually and on* behalf of all others similarly situated,

Plaintiff,

v

Case No. 2022CH00097

FILED

1/5/2022 4:31 PM IRIS Y. MARTINEZ

CIRCUIT CLERK

2022CH00097

Calendar, 16

16177509

COOK COUNTY, IL

NETRADYNE, INC.,

Defendant.

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff David Arendt ("Plaintiff"), individually and on behalf of all other persons similarly situated, by and through his undersigned counsel, brings this Class Action Complaint and Demand for Jury Trial against Defendant Netradyne, Inc. ("Netradyne") for its violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA"). Plaintiff alleges the following facts based upon personal knowledge as to himself and his own acts and experiences and, as to all other matters, upon information and belief.

NATURE OF THE ACTION

1. Plaintiff brings this action for damages and other legal and equitable remedies resulting from Defendant's unlawful capturing, collecting, storing, and using Plaintiff's and other similarly situated individuals' biometric identifiers¹ and biometric information² (collectively, "biometrics") without first obtaining informed written consent or providing the requisite data

¹ A "biometric identifier" is defined as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10

² "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." 740 ILCS 14/10

retention and destruction policies, in direct violation of BIPA.

2. Netradyne is a video analytics and software company headquartered in San Diego, California. Netradyne contracts with transportation companies, including those in Illinois, to integrate its services into their vehicles for the purpose of monitoring the equipment and its drivers. Netradyne's premier product, Driveri, is capable of simultaneously monitoring a vehicle's external conditions as well as its driver and is marketed as a safety tool.

3. Plaintiff is employed by Bob's Discount Furniture ("BDF") as a truck driver. BDF operates a fleet of trucks in Illinois which it uses to transport goods from its distribution centers to its retail establishments and customers' homes. BDF contracted with Netradyne to begin installing its Driveri system into its fleet of trucks in 2021 in order to protect the company against loss occurring from vehicle accidents.

4. Netradyne's Driveri is a multi-camera hardware device that is mounted on the windshield or dash of a vehicle. Driveri is purpose-built to capture video and assess it with vision-based artificial intelligence. Using these technologies, Driveri can continuously monitor and classify the driver's status as well as external variables like cars or road signs.

5. To monitor drivers, Driveri collects, *inter alia*, scans of the driver's face geometry and analyzes them to detect specific types of driver behavior—such as distracted or drowsy driving. The camera then uses its built-in cellular data link to upload the video, biometrics, and other incident data (*e.g.*, driver profile information, telematics information, etc.) to Netradyne's servers for storage. Netradyne set up the Driveri system in such a way that any biometrics collected through the Driveri system would also be collected and stored by Netradyne. The driver's employer is provided a login that allows the employer to review the data stored on Netradyne's servers, including driver and incident information.

FILED DATE: 1/5/2022 4:31 PM 2022CH00097

6. Uploading this data so that users can access it using the Netradyne customer portal is a core feature of Netradyne's product. However, this feature also provides Netradyne with access to the information for its own purposes. Every day, Netradyne adds new driver and trip data to its trove of information consisting of over 10 billion miles of driving data.

7. The act of scanning drivers' face geometry and storing the data on a Netradyne server exposes drivers' sensitive personal data to privacy risks. If the server is breached by an unauthorized third party, drivers' biometrics could be used to steal their identities or to track them without authorization.

8. The Illinois legislature understood this risk when it enacted BIPA, which imposes strict requirements that private entities must follow in conjunction with the collection of biometric identifiers or biometric information.

9. However, Netradyne fails to honor Illinois drivers' statutorily protected rights when they collect biometric data in violation of BIPA. Specifically, Defendant Netradyne violated and continues to violate BIPA because it:

- (i) failed to develop a publicly available retention schedule and guidelines for the destruction of biometrics;
- (ii) failed to inform drivers monitored by the Netradyne system that their biometrics would be collected and stored;
- (iii) failed to inform drivers monitored by the Netradyne system of the purpose and length of term for which the biometrics would be stored or used; and
- (iv) failed to obtain a written release from drivers whose face geometry was scanned and collected by its technology.

10. Plaintiff, on behalf of himself and the class as defined herein, brings this action to prevent Defendant from further violating the privacy rights of citizens in the State of Illinois and to recover statutory damages for Defendant's unauthorized collection, capture, storage, and use of

individuals' biometrics in violation of BIPA.

JURISDICTION AND VENUE

11. Netradyne is subject to the personal jurisdiction of this court pursuant to 735 ILCS 5/2-209 because it conducts business transactions in Illinois, both with BDF and, on information and belief, other companies that operate commercial fleets. Netradyne is also subject to the personal jurisdiction of this court because it has committed tortious acts in Illinois. Additionally, this court has jurisdiction over Plaintiff because Plaintiff resides in Illinois.

12. Venue is proper in Cook County because Defendant conducts business transactions in Illinois and has committed tortious acts in this County.

PARTIES

13. Plaintiff, David Arendt, is and has been at all relevant times a resident and citizen of Will County, Illinois. Plaintiff is employed as a driver for BDF.

14. Netradyne, Inc. is a software company incorporated in Delaware and headquartered in San Diego, California, and provides advanced vision technology software to companies in the transportation industry.

BACKGROUND

I. The Illinois Biometric Information Privacy Act

15. In 2008, the Illinois legislature enacted BIPA due to the "very serious need [for] protections for the citizens of Illinois when it [comes to their] biometric information." Illinois House Transcript, 2008 Reg. Sess. No. 276.

16. A "biometric identifier" is defined as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10.

17. In turn, "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." 740 ILCS 14/10.

18. BIPA makes it unlawful for a company to, *inter alia*, "collect, capture, purchase,

receive through trade, or otherwise obtain a person's or a customer's biometrics, 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."

740 ILCS 14/15(b).

19. Section 15(a) of BIPA also provides that:

A 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. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

Id. at 14/15(a).

20. In sum, BIPA is an informed consent statute that allows companies to collect, store,

and use biometrics so long as they make the relevant disclosures and obtain consent from individuals before doing so.

II. Defendant's Conduct Violates BIPA.

A. Defendant Collects Biometrics from Users of Driveri.

21. In 2021, BDF installed Netradyne's Driveri system across its fleet of trucks, including in the truck driven by Plaintiff.

22. Netradyne's Driveri system is a vision-based artificial intelligence system which analyzes video collected from a camera mounted on the interior windshield of trucks. This camera is mounted in the cab of the truck and aimed such that the lens will capture the driver and his or her behavior.

23. The camera system includes software technology which is capable of determining when a person is operating the vehicle, identifying that person, and assessing the person's movements and actions, as illustrated by numerous marketing materials published by Netradyne.

24. The monitoring system employed by Driveri scans the driver's face geometry locally on the Driveri device installed in the truck—in order to determine that a face exists within the camera's field of view or, in some cases, to identify the driver. The facial geometry collected is then sent to Netradyne to be stored on its servers.

25. But going further, the system can analyze the data that it captures and learn from it. Specifically, Netradyne's Driveri system is able to distinguish between different types of driver status—for example, focused driving, eyes on the road, or drowsiness—or specific actions that may cause distraction such as eating, drinking, or utilizing a mobile device as depicted in Figure 1. In Netradyne's words, its "advanced AI technology can assess distracted driving behaviors like drowsiness and texting while driving."



(Figure 1)

26. Netradyne's publicly available patent filings further detail the technical features of Netradyne's products. For example, patent filings made by Netradyne indicate that its technology can use facial recognition techniques to assess whether a given driver is among the list of authorized drivers for a particular vehicle. These patent filings also indicate that Netradyne's technology can capture the points on an individual's face and map them to understand where the driver is looking.

27. Moreover, Netradyne's filings with the Federal Communications Commission indicate that Driveri uses hardware that is purpose-built for on-device artificial intelligence and machine vision use cases like those described in Netradyne's patents.

28. The Driveri unit transmits the data it collects and derives to Netradyne's servers via a persistent 4G cellular data connection built into the unit. This data may be assigned to a specific individual's driver profile in the Netradyne system.

29. Netradyne stores this data on its servers, adding to its trove of data every day. The company currently claims to add over 700 million miles of driving data per month and that its system has collected and stored over 1 billion miles of driving data on its systems.

7

to or Dash "real beha beha

30. Netradyne provides an online portal, the Fleet Dashboard, which allows companies to organize and view the data Netradyne has collected from their trucks and drivers. The Fleet Dashboard purports to contain up-to-the-minute data about a company's entire fleet, allowing for "real-time alerts to ensure visibility to [*sic*] drivers' behavior that require [*sic*] action."

31. By collecting and storing scans of drivers' face geometry, Netradyne is able to harness artificial intelligence and biometric technology to monitor drivers for poor driving behavior and reduce the need for human review of hours of video streams. By applying its biometric-monitoring software in real-time to such large volumes of data, the product is able to pinpoint instances of driver error as they occur.

32. This system is only capable of providing these features because of Netradyne's ability to scan a driver's face geometry using its advanced machine vision system, store the data pulled from those scans, and process the data using artificial intelligence software.

B. Defendant Captures, Stores, and Uses Biometrics Absent Notice and Informed Written Consent.

33. As explained above, Defendant collects Plaintiff's and the putative class members' biometric identifiers and biometric information. Defendant further stores this data on its servers for future use.

34. BIPA clearly prohibits the collection of biometrics when the subject of the biometrics is deprived of the right to be informed of, and give written consent to, the capture of biometric data. Under BIPA, "[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... 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."

See 740 ILCS 14/15(b).

35. Netradyne did not inform Plaintiff and the putative class members it was collecting scans of their face geometry. Netradyne further never informed Plaintiff and the putative class members it was storing scans of their face geometry or biometric data derived therefrom.

36. Netradyne did not inform Plaintiff and the putative class members of the specific purpose or length of term for which this data would be collected, stored, or used.

37. Moreover, Netradyne never attempted to obtain a written release from Plaintiff or the putative class members to collect their sensitive biometric data.

38. The only information received by Plaintiff (and, on information and belief, the putative class members) was a notice from their employer that cameras would be installed in their vehicles and that the purpose of installing the cameras was to reduce costs of litigation from traffic accidents. Neither Plaintiff nor any of the putative class members received any information or notice that Netradyne was collecting their biometrics through the cameras installed in their vehicles.

39. Defendant violates Section 15(b) of BIPA because 1) it did not inform Plaintiff and other putative class members of the collection of their biometrics, the specific purpose for collection, and the term for collection, storage, and use, before collecting their biometrics; and 2) it did not obtain a written release to collect their biometrics before doing so.

C. Defendant Fails to Maintain Publicly Available Retention and Destruction Guidelines.

40. As explained above, Netradyne collects, stores, and uses Plaintiff's and putative class members' biometrics.

41. As a private entity engaged in the collection, capture, storage, and use of biometrics, BIPA requires Defendant to "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 the [biometrics] 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).

42. Netradyne hosts a publicly available privacy policy on its website, but neither the privacy policy, nor any other section of the website, mentions the collection, storage, and use of biometrics from drivers in any fashion, a retention schedule for Netradyne's collection of biometrics, or guidelines for the destruction of the collected biometric data. On information and belief, Netradyne has not established any policies or procedures for the retention and deletion of biometric data, let alone one that is publicly available. As a result, drivers of trucks equipped Netradyne's Driveri cameras and related software have no information as to whether or for how long this sensitive biometric data may be retained by Netradyne.

43. Additionally, not only does BIPA require an entity such as Netradyne to host the aforementioned publicly available policies, but it also requires private entities to comply with such policies. Without access to a policy explaining Netradyne's retention and deletion of biometrics, Plaintiff cannot know whether Netradyne will ever delete his biometric data. Netradyne's statements related to its storage of vast amounts of data only suggest that his biometric data has not and never will be deleted.

44. Netradyne's failure to establish and comply with the required written retention and deletion policy related to biometrics violates 740 ILCS 14/15(a).

FACTS SPECIFIC TO PLAINTIFF ARENDT

45. Plaintiff is a resident of the State of Illinois.

46. As part of his duties as an employee for BDF, Plaintiff operated a vehicle which was outfitted with a camera and software designed and implemented by Netradyne—specifically, a Driveri model D-210.

47. In the course of his employment, Plaintiff operated the vehicle outfitted with the aforementioned Netradyne Driveri unit in the State of Illinois.

48. Consequently, Plaintiff was required to submit to Netradyne's scans of his face geometry while in the State of Illinois.

49. Because Netradyne collects geolocation information as part of its tracking software, the company knew or reasonably should have known of Plaintiff's location while his face geometry was scanned. As such, Netradyne knew, actually or constructively, that it was collecting biometrics from the Plaintiff while he was in the State of Illinois.

50. Netradyne did not inform Plaintiff it was capturing his biometrics or the purpose and length of term for such collection. Nor did Netradyne obtain Plaintiff's written consent prior to capturing his biometrics; in fact, Netradyne has never even presented Plaintiff with any type of written consent form related to biometrics. Plaintiff never consented, agreed, or gave permission to Defendant for the collection, storage, or use of his biometrics for any purpose.

51. Moreover, Defendant never established or provided Plaintiff access to a retention schedule and guidelines for permanently destroying his biometric data once its purpose for his biometrics was completed (or within three years of his last interaction with Netradyne).

11

52. Upon information and belief, Defendant continues to retain Plaintiff's biometric data beyond the intended purpose for collection and has not deleted his biometric data.

CLASS ALLEGATIONS

53. Plaintiff brings this action pursuant to Illinois Code of Civil Procedure Section 2-

801 on behalf of the following class of similarly situated individuals, defined as follows:

All residents of the State of Illinois who had their biometrics collected, captured, received, or otherwise obtained by Netradyne while residing in Illinois.

54. <u>Numerosity</u>: The number of persons within the Class is substantial, believed to amount to hundreds of persons or more. It is, therefore, impractical to join each member of the Class as a named Plaintiff. Accordingly, utilization of the class action mechanism is the most economically feasible means of determining and adjudicating the merits of this litigation. Moreover, the Class is ascertainable and identifiable from Defendant's records.

55. <u>Commonality & Predominance</u>: There are well-defined common questions of fact and law that exist as to all members of the Class and that predominate over any questions affecting only individual members of the Class. These common legal and factual questions, which do not vary from Class member to Class member, and which may be determined without reference to the individual circumstances of any class member, include, but are not limited to, the following:

- (a) whether Defendant captured, collected, or otherwise obtained Plaintiff's and the Class's biometrics;
- (b) whether Defendant properly informed Plaintiff and the Class that it captured, collected, used, and stored their biometrics;
- (c) whether Defendant obtained a written release to capture, collect, use, and store Plaintiff's and the Class's biometrics;
- (d) whether Defendant developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometrics when the initial purpose for

collecting or obtaining such biometrics has been satisfied or within three years of their last interaction, whichever occurs first;

- (e) whether Defendant complies with any such written policy (if one exists);
- (f) whether Defendant used Plaintiff's and the Class's face scans to identify them;
- (g) whether Defendant has sold, leased, traded, or profited from Plaintiff's and the Class's biometrics;
- (h) whether Defendant has disclosed, redisclosed, or otherwise disseminated Plaintiff's and the Class's biometrics without consent; and
- (i) whether Defendant's violations of BIPA were committed intentionally, recklessly, or negligently.

56. <u>Adequate Representation</u>: Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Class and have the financial resources to do so. Neither Plaintiff nor his counsel have any interest adverse to those of the other members of the Class.

57. <u>Appropriateness</u>: 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 all members of the Class is impracticable. The damages suffered by the individual members of the Class are likely to have been small relative to the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's wrongful conduct. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendant's misconduct. Even if members of the Class could sustain such

individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered, and uniformity of decisions will be ensured.

CLAIMS FOR RELIEF

COUNT I VIOLATION OF 740 ILCS 14/15(a) Failure to Develop Written Retention Schedule and Destruction Guidelines

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

59. BIPA mandates that companies in possession of biometric data establish and maintain a satisfactory biometric data retention—and, importantly, deletion—policy. Specifically, those companies must: (i) develop a written policy establishing a retention schedule and guidelines for permanent deletion of biometric data (at most three years after the company's last interaction with the individual); (ii) make that written policy publicly available, and (iii) actually adhere to that retention schedule and actually delete the biometric information. *See* 740 ILCS 14/15(a)

60. Netradyne is corporation and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

61. Plaintiff and the Class are individuals who had their "biometric identifiers" (in the form of their face geometry) collected by Netradyne, as explained in detail in Section II. *See id*.

62. Plaintiff's and the Class's biometric identifiers or information based on those biometric identifiers were, or can be, used to identify them, constituting "biometric information" as defined by BIPA. *See id*.

14

63. Netradyne contracts with BDF and other transportation companies to supply its cameras, software, and surveillance service in order to monitor drivers during their employment.

64. Netradyne provides cameras to BDF and other transportation companies, installs or assists in the installation of its cameras in trucks, leases its surveillance software to BDF and other transportation companies, provides servicing and analysis of data obtained from its cameras and software, and stores the data obtained from its cameras and software on Netradyne's servers.

65. Netradyne obtained and stored Plaintiff's and the Class's biometric identifiers. On information and belief, Netradyne maintains custody and control of the biometric data it possesses on servers accessible by it.

66. Despite obtaining and possessing biometric information in violation of BIPA, Netradyne violated 740 ILCS 14/15(a) by failing to publicly provide a retention schedule or guidelines for permanently destroying drivers' biometric identifiers and biometric information.

67. Netradyne hosts a publicly available privacy policy but does not include a written retention schedule or guidelines for the destruction of biometric data anywhere in this policy or anywhere else available for review by the public. In fact, Netradyne's privacy policy is silent regarding the collection of biometrics.

68. On behalf of himself and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with BIPA's requirements for the possession of biometrics as described herein; (3) statutory damages of \$5,000 for each intentional and/or reckless violation of BIPA or, in the alternative, statutory damages of \$1,000 for each negligent violation of BIPA; and (4) reasonable attorneys' fees and costs and other litigation expenses. *See* 740 ILCS 14/20.

COUNT II VIOLATION OF 740 ILCS 14/15(b) Failure to Obtain Informed Written Consent and Release Before Obtaining Biometrics

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

70. BIPA requires companies to obtain informed written consent from employees before acquiring their biometric data. Specifically, BIPA makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless [the entity] 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, and (3) receives a written release executed by the subject of the biometric identifier or biometric information" 740 ILCS 14/15(b) (emphasis added).

71. Netradyne is corporation and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

72. Plaintiff and the Class are individuals who had their "biometric identifiers" (in the form of their face geometry) collected by Netradyne, as explained in detail in Section II. *See id*.

73. Plaintiff's and the Class's biometric identifiers or information based on those biometric identifiers were, or can be, used to identify them, constituting "biometric information" as defined by BIPA. *See id*.

74. Defendant obtained and stored Plaintiff's and the Class's biometric identifiers. On information and belief, Defendant maintains custody and control of the biometric data it possesses on servers owned or accessible by it.

75. Defendant failed to comply with the mandates of Section 15(b) by:

FILED DATE: 1/5/2022 4:31 PM 2022CH00097

16

- a) Recklessly and/or negligently failing to inform Plaintiff and the Class in writing that their biometric identifiers and biometric information were being collected and stored, 740 ILCS 14/15(b)(1);
- b) Recklessly and/or negligently failing to inform Plaintiff and the Class in writing of the specific purpose and length of time for which their biometric identifiers or biometric information was being collected and stored, 740 ILCS 14/15(b)(2); and
- c) Recklessly and/or negligently failing to obtain written releases from Plaintiff and the Class before they collected, used, and stored their biometric identifiers and biometric information, 740 ILCS 14/15(b)(3).

76. By systematically and automatically collecting, storing, and using Plaintiff's and the Classes' biometric identifiers and biometric information as described herein, Defendant violated Plaintiff's and the Class's rights to privacy in their biometric identifiers or biometric information as set forth in BIPA, 740 ILCS 14/1, *et seq*.

77. On behalf of himself and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with BIPA's requirements for the collection, storage, use and dissemination of biometrics as described herein; (3) statutory damages of \$5,000 for each intentional and/or reckless violation of BIPA or, in the alternative, statutory damages of \$1,000 for each negligent violation of BIPA; and (4) reasonable attorneys' fees and costs and other litigation expenses. *See* 740 ILCS 14/20.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the proposed 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 his counsel as Class Counsel;
- B. Declaring that Defendant's actions, as set out above, violate BIPA, 740 ILCS 14/1, *et seq.*;
- C. Awarding statutory damages of \$5,000.00 for each and every intentional and reckless violation of BIPA, or alternatively, statutory damages of \$1,000.00 for each and every negligent violation of BIPA;
- D. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class, including, *inter alia*, an Order requiring Defendant to comply with BIPA;
- E. Awarding Plaintiff and the Class their reasonable attorneys' fees and costs and other litigation expenses;
- F. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and
- G. Awarding such other and further relief as equity and justice may require.

JURY TRIAL

Plaintiff David Arendt requests a trial by jury of all claims that can be so tried.

Respectfully submitted,

DAVID ARENDT, individually and on behalf of all others similarly situated,

Dated: January 5, 2022

By: <u>/s/Schuyler Ufkes</u> One of Plaintiff's Attorneys

J. Eli Wade-Scott ewadescott@edelson.com Schuyler Ufkes sufkes@edelson.com EDELSON PC 350 North LaSalle Street, 14th Floor Chicago, Illinois 60654 Tel: 312.589.6370 Fax: 312.589.6378 Firm ID: 62075

Randall K. Pulliam* rpulliam@cbplaw.com David F. Slade* dslade@cbplaw.com CARNEY BATES AND PULLIAM, PLLC 519 West 7th Street Little Rock, Arkansas 72201 Telephone: (501) 312-8500

*Admission pro hac vice to be sought

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: <u>Netradyne Hit with Privacy Class Action</u> <u>Over In-Vehicle Driver Facial Scans</u>