IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS

JOSHUA LEWIS, JAMES CAVANAUGH, and NATHANIEL TIMMONS, *individually and on behalf of all others similarly situated,* Plaintiffs, v LYTX, INC. Defendant.	Case No. 3:22-CV-00046-NJR

AMENDED CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiffs Joshua Lewis, James Cavanaugh, and Nathaniel Timmons ("Plaintiffs"), individually and on behalf of all other persons similarly situated, by and through undersigned counsel, bring this amended class action lawsuit for violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA"), against Defendant Lytx, Inc. ("Lytx" or "Defendant").[1] Plaintiffs allege the following facts based upon personal knowledge and/or the investigation of his counsel:

NATURE OF THE ACTION

1. Plaintiffs bring this action for damages and other legal and equitable remedies resulting from the illegal actions of Defendant in capturing, collecting, storing, using, and profiting

[1] Plaintiff Lewis's original complaint included allegations against Defendant Maverick Transportation, Inc. ("Maverick"). Mr. Lewis and Maverick fully resolved those claims on March 9, 2023, when the Court granted final approval of a class action settlement between them and Defendant Maverick was dismissed from the case. Dkt. 63.

from Plaintiffs' and other similarly situated individuals' biometric identifiers[2] and biometric information[3] (collectively, "biometrics") without first obtaining informed written consent or providing the requisite data retention and destruction policies, in direct violation of BIPA.

2. Lytx, Inc. is a video telematics and fleet management systems corporation based out of San Diego, California and provides video and analytics services to the transportation industry. Lytx employs a robust suite of technologies to provide services to its transportation clients, including sensors which monitor the location and movement of the truck itself, the truck's position in relation to other vehicles of objects on the road, and cameras which monitor and record video of both the inside of the cab and the outside of the vehicle.

3. Lytx's premier technology, however, is its machine vision and artificial technology capabilities—referred to by Lytx is its "MV+AI system" or "MV+AI." Lytx employs this MV+AI technology in its SF-300 DriveCam ("DriveCam"), a camera which videos the interior of the cab of the truck in order to monitor the driver. But the DriveCam does more than simply record images; in conjunction with the MV+AI, the DriveCam scans the driver's face geometry and harnesses those biometric data points by feeding them into sophisticated algorithms that identify the driver's actions, in what amounts to constant AI surveillance. *See* Exhibit 1.

4. Lytx contracted with various transportation companies, including Maverick in 2020, to incorporate its MV+AI-enabled DriveCam into trucks. Plaintiff Lewis was a truck driver for Maverick, and during the course of his employment drove many times while being recorded by the DriveCam system, and in each instance had his face geometry collected and captured by

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

[3] "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.

Lytx in violation of BIPA.

5. The implementation of this system is problematic because the DriveCam unacceptably violates the rights of truck drivers by scanning their faces and acquiring their face geometry and other biometrics in violation of their statutorily protected rights.

6. Lytx's technology is employed by more than 4,000 fleets across the country, and over the past 20 years it has continuously gathered data which it uses to program new software products and services. Lytx claims to hold data based on over *100 billion miles of driving* and continues adding information to a "vast and ever-growing database of driving data we use to refine the accuracy and effectiveness of our solutions."[4]

7. The act of scanning of drivers' face geometry and storing those collected biometrics in a Lytx facility exposes drivers' sensitive personal data to privacy risks. If a Lytx server becomes compromised through a data security breach, sensitive personal information based on the scans of these drivers' face geometry could be used to steal their identities or to track them.

8. The Illinois legislature understood this risk when it enacted the Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA"), which imposes strict requirements private entities must follow in conjunction with the collection of biometric identifiers or biometric information.

9. However, Lytx failed to honor drivers' statutorily protected rights when it collected biometric data in violation of BIPA. Defendant violated BIPA because it

(i) failed to develop a publicly available retention schedule and guidelines for the destruction of biometrics; and

(ii) failed to inform drivers of the purpose and length of term for which the

[4] https://www.lytx.com/en-us/about-us/our-story (attached as Exhibit 2)

biometrics would be stored or used and failed to obtain a written release from them.

10. Lytx further violates BIPA because it expressly profits from the collection of the drivers' biometrics when it uses its trove of biometrics stored on its servers to engineer and manufacture new products for sale and to market its existing products to new customers.

11. Plaintiffs, on behalf of themselves and the class as defined herein, bring 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 anduse of individuals' biometrics in violation of BIPA.

JURISDICTION AND VENUE

12. Defendant Lytx is subject to the personal jurisdiction of the Court because it is registered to do business with the State of Illinois, regularly transacts business within the State of Illinois, and has purposefully availed itself of the laws of Illinois for the specific transactions at issue. Further, the biometrics that give rise to this lawsuit were collected by Defendant from drivers of trucks outfitted with Lytx technology within the State of Illinois.

13. Venue is proper in this Court because Defendant does substantial business in this District and a substantial part of the events giving rise to Plaintiffs' claims took place within this District because Plaintiff Lewis's biometrics were collected in this District.

PARTIES

14. Plaintiff Joshua Lewis was, and has been at all relevant times, a resident and citizen of Madison County, Illinois, and an employee as a driver for Maverick.

15. Plaintiff James Cavanaugh was, and has been at all relevant times, a resident and citizen of Illinois.

16. Plaintiff Nathaniel Timmons was, and has been at all relevant times, a resident and citizen of Illinois.

17. Defendant Lytx is a software company based in San Diego, CA, and provides video and analytics software services to companies in the transportation industry. Specifically, Lytx develops and leases to its customers technology which monitors transportation equipment and the operators of that equipment to maximize efficiency and safety. During the relevant period, Lytx contracted with trucking companies to facilitate MV+AI-enabled DriveCam installations across its fleet to monitor drivers.

BACKGROUND

I. The Illinois Biometric Information Privacy Act

18. In 2008, Illinois 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.

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

20. 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.

21. 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).

22. 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).

23. Further, BIPA prohibits a "private entity in possession of a biometric identifier or biometric information" from "sell[ing], leas[ing], trad[ing], or otherwise profit[ing] from a person's or a customer's biometric identifier or biometric information." 740 Ill. Comp. Stat. Ann. 14/15(c).

24. Nor may a private entity "disclose, redisclose, or otherwise disseminate an individual's biometrics absent written consent." 740 ILCS 14/15(d).

25. Finally, BIPA places significant security requirements on private entities that acquire individuals' biometrics, stating that they must: "(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).

II. Defendant's BIPA-Violative Conduct

A. Defendant Captures Biometrics Absent Informed Written Consent

i. Defendant Collects Biometrics

26. BIPA clearly prohibits the collection of biometrics when the subject of the biometrics is deprived of the right to be informed of, and 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).

27. Lytx offers a suite of technologies designed to enhance the abilities of transportation companies to manage their fleets. One particular system is AI Risk Detection, which "identif[ies] unsafe driving behavior and prompts drivers with in-cab alerts to help them self-

correct in the moment."[5] When paired with Machine Vision the technology can be used to notify transportation companies "when driving behaviors like inattentive driving, speeding, failure to wear a seat belt, smoking, eating, drinking…and using handheld devices occur."[6]

28. The upshot is that the DriveCam uses MV+AI technology to constantly monitor and analyze the goings-on inside Class members' vehicles.

29. This constant monitoring fundamentally relies on face detection technology. First, an algorithm is "trained" to recognize faces in a video after having been fed hundreds of thousands of images of drivers and their behaviors. Video is then reviewed and tagged by humans; tagged video is then again fed into the algorithm in order to teach it which data should be considered "relevant." *See* Exhibit 4.

30. That algorithm is then deployed in the technology behind the DriveCam. The camera scans a driver's face geometry, identifying a host of unique points around multiple regions of the driver's face (*i.e.*, each eye, the mouth, the nose, the lips, etc.). Once the DriveCam has successfully detected a driver is present (via a scan, *inter alia*, of face geometry), the DriveCam then applies the MV+AI algorithm described *infra*, and identifies not only the presence of the driver, but also what the driver is *doing* in real time.

31. Thus, the DriveCam continuously "watches" the driver on whom it is trained; scans the driver's face geometry; analyzes the face geometry scans to determine whether the driver is eating, drinking, looking at a mobile device, smoking, or engaging in other prohibited behavior; and submits an alert to the driver and his or her employer upon making a judgment that the observed behavior (identified via biometric scans) are consistent with its database of video and

[5] https://www.lytx.com/en-us/fleet-management/fleet-safety (attached as Exhibit 3)
[6] *Id.*

images which are tagged as being sufficiently relevant events.[7] Per Lytx, the machine vision component of the MV+AI Camera "sees and recognizes," while the artificial intelligence component of the technology "interprets and decides."

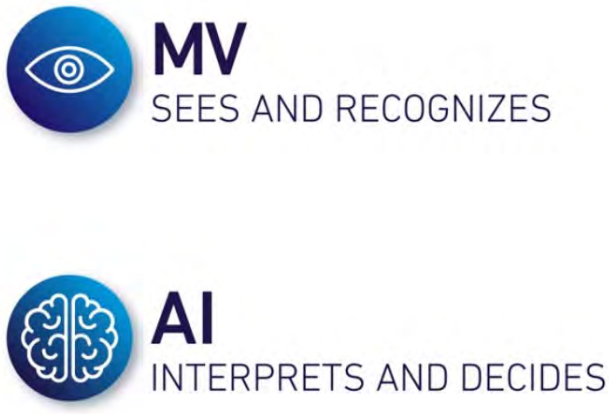

Figure 1[8]

[7] Fleet Safety, *supra*
[8] https://www.lytx.com/en-us/about-us/our-technology/machine-vision-artificial-intelligence (attached as Exhibit 5)

32. The following illustrations, from Lytx, demonstrate the functionality of the DriveCam's face-scanning technology:

Figure 2[9]

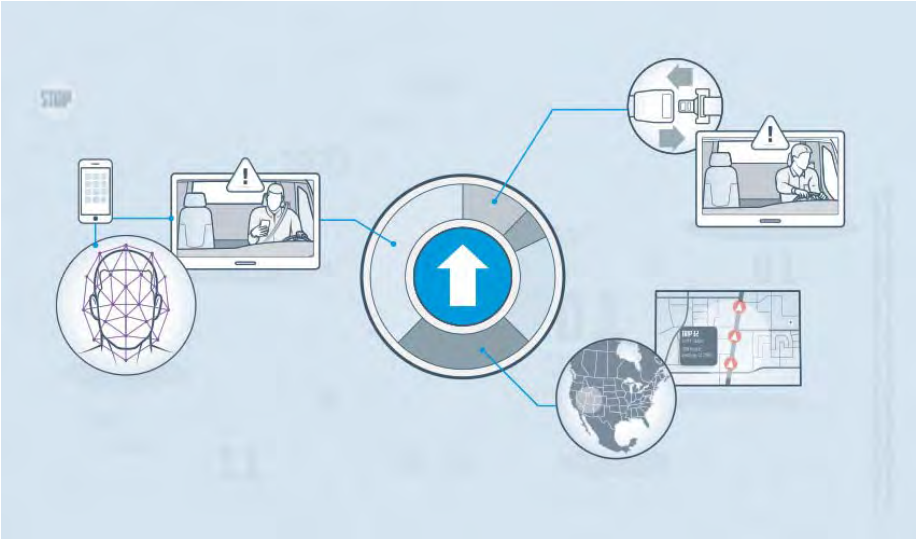

Figure 3[10]

[9] https://www.lytx.com/en-us/fleet-management/features/risk-id-without-recording (attached as Exhibit 6)
[10] Demystifying MV+AI, *supra*

Figure 4[11]

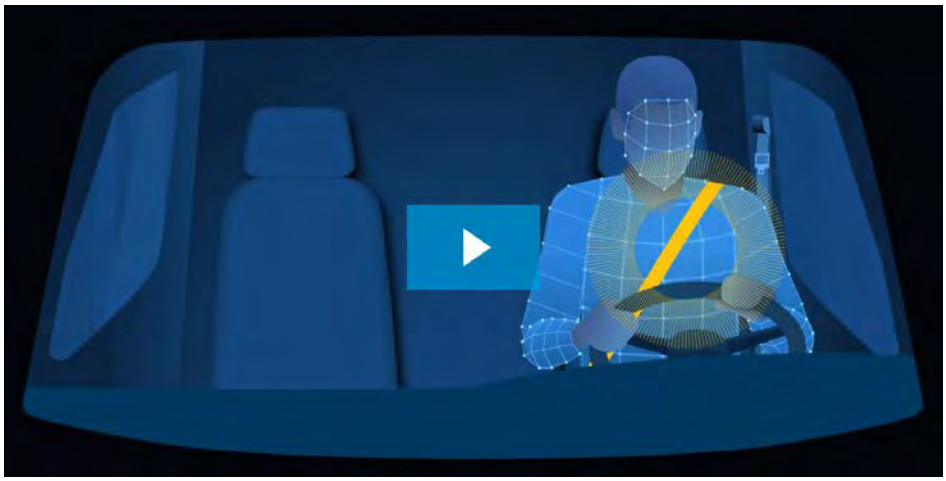

Figure 5[12]

[11] Our Technology, *supra*
[12] *Id.*

Figure 6[13]

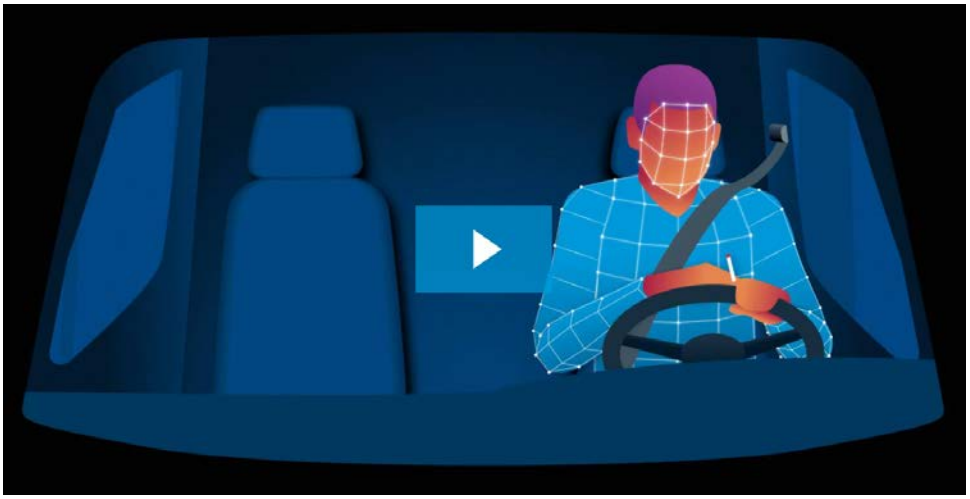

Figure 7[14]

33. Face detection "is the first and essential step for face recognition," and is used as a preliminary step to detect faces in images. It is a part of object detection and is used in many areas, including biometrics.[15] Face detection "is used to detect faces in real time for surveillance and tracking of [a] person or objects."[16]

[13] *Id*.
[14] *Id*.
[15] *See*, Divyanch Dwivedi, *Face Detection for Beginners*, Towards Data Science (available at https://towardsdatascience.com/face-detection-for-beginners-e58e8f21aad9) (attached as Exhibit 7)
[16] *Id*.

34. Specifically, face detection technology uses algorithms and machine learning to find human faces within larger images.[17] Face detection algorithms start by scanning the collected image for human eyes, one of the easiest features to detect. The algorithm then attempts to detect eyebrows, the mouth, nose, nostrils, and the iris.[18] *E.g.*

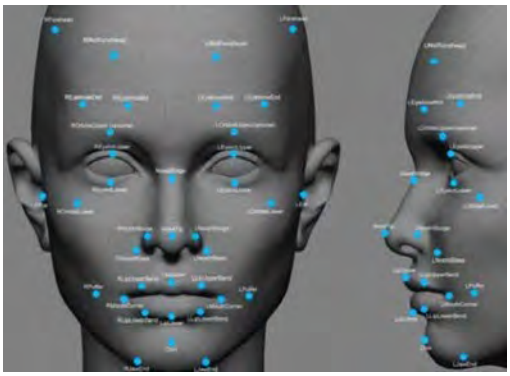

Figure 8[19]

35. Once the algorithm classifies a sufficient number of data points in the scanned image as belonging to a face (i.e., eyes mouth, nose, nostrils, and iris), it applies additional tests to confirm that it has, in fact, detected a face.[20]

[17] *See, generally*, Corrine Bernstein, *Face Detection*, Search Enterprise AI (available at https://searchenterpriseai.techtarget.com/definition/face-detection) (attached as Exhibit 8)
[18] *Id.*; *see, also*, OpenCV, *Cascade Classifier*, (available at https://docs.opencv.org/3.4/db/d28/tutorial_cascade_classifier.html) (attached as Exhibit 9)
[19] Keval Dohsi, *Face Detection using Raspberry Pi and Smartphone*, Hackster.io (available at https://www.hackster.io/keval-doshi/face-detection-using-raspberry-pi-and-smartphone-19f1f2) (attached as Exhibit 10) (describing how to create facial detection technology using OpenCV)
[20] *See, generally*, Bernstein, *Face Detection*, fn 8, *supra*.

Figure 9 [21]

36. Once trained, the model extracts specific features, which are then stored in a file so that features from new images can be compared with the previously stored features at various stages. If the image under study passes through each stage of the feature comparison, then a face has been detected and operations can proceed.[22]

37. The above-described procedures rely on "face landmark detection," generally, in order to identify the specific landmarks on a face (eyes, nose, cheeks, etc.) for face detection. But face landmark detection is capable of even more sophisticated analyses of the face geometry scans it acquires, enabling Lytx to uniquely identify actions taken by the scanned individual, such as smoking, or eating or drinking, or using a mobile device.

38. Face detection algorithms like Lytx's are trained by feeding the algorithm a "set of delegate training face images to find out face models."[23] This approach, called the Appearance-Based Method "rel[ies] on techniques from statistical analysis and machine learning to find the

[21] OpenCV, *Cascade Classifier*, fn 9, *supra*.
[22] *See, generally*, Bernstein, *Face Detection*, fn 8, *supra*.
[23] *See*, Divyanch Dwivedi, *supra*

relevant characteristics of face images."[24]

39. Lytx provides the DriveCam, the MV+AI software, and its services, which includes human reviewers, to transportation companies, and as part of this agreement, stores the data at its facilities where further analysis and AI training occurs. Thus, Lytx actively and continuously scans and collects the face geometry of the driver to determine whether his face indicates he is engaged in prohibited conduct.

ii. Defendant Failed to Obtain Written Consent

40. Defendant collected, and has collected, Plaintiffs' and the putative Class members' biometric identifiers and biometric information when its technology scans their face geometry.

41. However, at no point are Class members informed of the collection of their biometric identifiers or biometric information, and Class members are never informed in writing the purpose or length of term for which their biometrics are being collected and stored, and they are never requested or invited to provide written consent for Defendant to collect their biometrics.

42. Lytx provided no written information to Class members, and further purports to disclaim any responsibility for informing the subjects of its surveillance as to what it collects. The Lytx Privacy Policy expressly disclaims any "responsibility for the privacy or data security practices of [its] clients…" and further excludes from the scope of its Privacy Policy the processing of "Personal Information" in the role of a service provider on behalf of our clients."[25]

43. Without providing information to Class members in writing pertaining to the collection of biometrics via the DriveCam, and without obtaining informed consent to do so, Defendant violated BIPA.

[24] *Id.*
[25] Lytx Privacy Policy, https://www.lytx.com/en-us/privacy-policy (attached as Exhibit 11)

B. Defendant Failed to Maintain Publicly Available Retention and Destruction Guidelines

44. As private entities engaged in the collection, capture, storage, and use of biometric identifiers and biometric information, 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)

45. Lytx designed its DriveCam and the MV+AI technology and contracted with trucking companies to install and operate its DriveCam system for the purpose of scanning the face geometry of employees and storing the data at its facilities.

46. Lytx hosts a privacy policy on its website, but expressly "excludes from coverage under its Privacy Policy the processing of Personal Information in the role of a service provider on behalf of [its] clients."[26]

47. As a private entity that collect biometrics, Defendant violated BIPA by failing to establish a publicly available retention schedule and destruction guidelines for the biometric identifiers or biometric information of truck drivers.

C. Lytx Profits from the Collection of Biometrics

48. BIPA expressly prohibits behavior which would create a market for biometrics. "No 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).

[26] *Id.*

49. Lytx develops and operates technology systems, including its DriveCam, for use in the transportation industry, and said technology is fundamentally based on capturing the biometrics of truck drivers. Lytx collects this sensitive data and stores it along with data collected from over "100 billion miles of driving" and uses the data to improve the effectiveness of its software.[27]

50. Moreover, Lytx sells its biometrics-collecting system to companies with claims that by using its services "[o]ur clients can realize significant returns on investment by lowering operative and insurance costs."[28]

51. Lytx strategically markets its products based on its acquisition of biometrics in violation of BIPA. According to Lytx, the precision of its technology at predicting and preventing undesired driving behaviors is the fact it can draw from such a large stockpile of data which it stores on its premises for continual and repeated reviews using human analysis. Lytx claims it "uses innovative technology to reliably uncover risk" and its technology is superior to its competitors because it holds "the best data."[29] Going further: "The combination of high data volume and accuracy means that our MV+AI algorithms have better raw materials to work with, helping to deliver more precise results so that you aren't wading through an ocean of irrelevant information."[30]

52. Lytx not only uses biometrics to create new products and software to sell, but explicitly markets its products and services based on the collection of biometrics.

53. Lytx is engaged in a market based on the use and sale of biometrics in violation of BIPA.

---

[27] https://www.lytx.com/en-us/news-events/press-release/2018/lytx-presents-state-of-the-data (attached as Exhibit 12).
[28] Our Story, *supra*
[29] Demystifying, *supra*
[30] *Id.*

III. Plaintiffs' Experience

A. Plaintiff Lewis

54. As part of his duties as an over-the-road driver for Maverick, Plaintiff Lewis's truck was retrofitted with the DriveCam in or around October 2020.

55. Plaintiff Lewis is an Illinois resident whose biometrics were scanned by the DriveCam and by Lytx's MV+AI software while in the state of Illinois, with full knowledge of Maverick and Lytx, and at Maverick's direction. Maverick assigned Plaintiff Lewis routes as an over-the-road driver which regularly directed him to operate his truck within the state of Illinois multiple times per week. Defendant Lytx was also aware its software was utilized upon Plaintiff Lewis within the State of Illinois because Lytx tracks the geolocation of its cameras as part of its data collection and analysis service.[31] Thus, Defendant knew Plaintiff Lewis's physical location while the surveillance technology was in use.

56. In the course of his employment for Maverick, Plaintiff Lewis was required to undergo the DriveCam's scanning procedures in a manner substantially similar—if not identical—to the processes set forth above.

57. In so doing, Defendant Lytx's technology scanned, captured, collected and obtained Plaintiff Lewis's face geometry and stored his biometrics.

58. Neither Maverick nor Lytx informed Plaintiff Lewis they were capturing and collecting his biometrics or the purpose and length of time for such collection, nor did Defendant obtain Plaintiff Lewis's written consent beforecapturing his biometrics. Plaintiff Lewis never consented, agreed, or gave permission—written or otherwise—to Defendant for the collection, storage, or use of his biometrics.

[31] *Id.*

59. Likewise, Defendant never provided Plaintiff Lewis with the requisite statutory disclosures nor an opportunity to prohibit or to prevent the collection, storage or use of his biometrics.

60. Moreover, despite BIPA's clear prohibition against the sale, lease, trade, or otherwise profiting from the collection of biometrics, Lytx collected Plaintiff Lewis's biometrics for storage and analysis in a Lytx facility along with a collection of "over 100 billion miles of driving" for the purpose of "tagging them for potentially hazardous behaviors and conditions."[32] Thus, Defendant Lytx collected Plaintiff Lewis's biometrics to be used for the purposes of training and informing existing technologies and developing and marketing new products for sale by Lytx.

61. Plaintiff Lewis was deprived of his right to protect his biometrics when Defendant captured his biometrics without informing him of this practice, without obtaining his informed written consent to do so, and by exploiting Plaintiff Lewis's most sensitive personal data for profit. In so doing, Defendant invaded Plaintiff Lewis's statutorily protected right to privacy in his biometrics.

B. Plaintiff Cavanaugh

62. As part of his duties as an over-the-road driver for Quikrete, Plaintiff Cavanaugh's truck was retrofitted with the DriveCam.

63. Plaintiff Cavanaugh is an Illinois resident whose biometrics were scanned by the DriveCam and by Lytx's MV+AI software while in the state of Illinois, with full knowledge of Lytx. Mr. Cavanaugh drove his truck for his employer, Quikrete, within Illinois. Defendant Lytx was also aware its software was utilized upon Plaintiff Cavanaugh within the State of Illinois because Lytx tracks the geolocation of its cameras as part of its data collection and analysis

[32] *Id.*

service.[33] Thus, Defendant knew Plaintiff Cavanaugh's physical location while the surveillance technology was in use.

64. In the course of his employment, Plaintiff Cavanaugh was required to undergo the DriveCam's scanning procedures in a manner substantially similar—if not identical—to the processes set forth above.

65. In so doing, Defendant Lytx's technology scanned, captured, collected and obtained Plaintiff Cavanaugh's face geometry and stored his biometrics.

66. Lytx did not inform Plaintiff Cavanaugh that it was capturing and collecting his biometrics or the purpose and length of time for such collection, nor did Defendant obtain Plaintiff Cavanaugh's written consent before capturing his biometrics. Plaintiff Cavanaugh never consented, agreed, or gave permission—written or otherwise—to Defendant for the collection, storage, or use of his biometrics.

67. Likewise, Defendant never provided Plaintiff Cavanaugh with the requisite statutory disclosures nor an opportunity to prohibit or to prevent the collection, storage or use of his biometrics.

68. Moreover, despite BIPA's clear prohibition against the sale, lease, trade, or otherwise profiting from the collection of biometrics, Lytx collected Plaintiff Cavanaugh's biometrics for storage and analysis in a Lytx facility along with a collection of "over 100 billion miles of driving" for the purpose of "tagging them for potentially hazardous behaviors and conditions."[34] Thus, Defendant Lytx collected Plaintiff Cavanaugh's biometrics to be used for the purposes of training and informing existing technologies and developing and marketing new products for sale by Lytx.

[33] *Id.*
[34] *Id.*

69. Plaintiff Cavanaugh was deprived of his right to protect his biometrics when Defendant captured his biometrics without informing him of this practice, without obtaining his informed written consent to do so, and by exploiting Plaintiff Cavanaugh's most sensitive personal data for profit. In so doing, Defendant invaded Plaintiff Cavanaugh's statutorily protected right to privacy in his biometrics.

C. Plaintiff Timmons

70. As part of his duties as an over-the-road driver for Gemini Motor Transport L.P. ("GMT"), Plaintiff Timmons's truck was retrofitted with the DriveCam.

71. Plaintiff Timmons is an Illinois resident whose biometrics were scanned by the DriveCam and by Lytx's MV+AI software while in the state of Illinois, with full knowledge of Lytx. Mr. Cavanaugh drove his truck for his employer, GMT, within Illinois, beginning in 2020. Defendant Lytx was also aware its software was utilized upon Plaintiff Timmons within the State of Illinois because Lytx tracks the geolocation of its cameras as part of its data collection and analysis service.[35] Thus, Defendant knew Plaintiff Timmons's physical location while the surveillance technology was in use.

72. In the course of his employment, Plaintiff Timmons was required to undergo the DriveCam's scanning procedures in a manner substantially similar—if not identical—to the processes set forth above.

73. In so doing, Defendant Lytx's technology scanned, captured, collected and obtained Plaintiff Timmons's face geometry and stored his biometrics.

74. Lytx did not inform Plaintiff Timmons that it was capturing and collecting his biometrics or the purpose and length of time for such collection, nor did Defendant obtain Plaintiff

[35] *Id.*

Timmons's written consent beforecapturing his biometrics. Plaintiff Timmons never consented, agreed, or gave permission—written or otherwise—to Defendant for the collection, storage, or use of his biometrics.

75. Likewise, Defendant never provided Plaintiff Timmons with the requisite statutory disclosures nor an opportunity to prohibit or to prevent the collection, storage or use of his biometrics.

76. Moreover, despite BIPA's clear prohibition against the sale, lease, trade, or otherwise profiting from the collection of biometrics, Lytx collected Plaintiff Timmons's biometrics for storage and analysis in a Lytx facility along with a collection of "over 100 billion miles of driving" for the purpose of "tagging them for potentially hazardous behaviors and conditions."[36] Thus, Defendant Lytx collected Plaintiff Timmons's biometrics to be used for the purposes of training and informing existing technologies and developing and marketing new products for sale by Lytx.

77. Plaintiff Timmons was deprived of his right to protect his biometrics when Defendant captured his biometrics without informing him of this practice, without obtaining his informed written consent to do so, and by exploiting Plaintiff Timmons's most sensitive personal data for profit. In so doing, Defendant invaded Plaintiff Timmons's statutorily protected right to privacy in his biometrics.

CLASS ALLEGATIONS

78. Plaintiffs bring this action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of a class of similarly situated individuals ("the Class"), defined as follows:

> All individuals who, while present in the State of Illinois, operated a vehicle equipped with a DriveCam, and for whom MV+AI was

[36] *Id.*

used to predict distracted driving behaviors, between October 12, 2016 and the earlier of Preliminary Approval[37] or January 1, 2025.

79. Excluded from the Class are: (a) any Judge or Magistrate Judge presiding over this action and members of their staff, as well as members of their families; (b) Defendant, Defendant's predecessors, parents, successors, heirs, assigns, subsidiaries, and any entity in which Defendant or its parents have a controlling interest, as well as Defendant's current or former employees, agents, officers, and directors; (c) persons who properly execute and file a timely request for exclusion from the Class; (d) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (e) counsel for Plaintiffs and Defendant; and (f) the legal representatives, successors, and assigns of any such excluded persons.

80. **Numerosity**: the number of persons within the tens-of-thousands. 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.

81. **Commonality & Predominance**: 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 Plaintiffs' and Class members' biometrics;

(b) whether Defendant properly informed Plaintiffs and the Class that it captured, collected, used, and stored their biometrics;

[37] Plaintiffs are herewith moving for preliminary approval of a class action settlement with Lytx.

(c) whether Defendant obtained a written release to capture, collect, use, and store Plaintiffs' and Class members' biometrics;

(d) whether Defendant sold, leased, traded, or profited from Plaintiffs' and Class members' biometrics;

(e) whether Defendant disclosed, redisclosed, or otherwise disseminated Plaintiffs' and Class members' biometrics absent consent; and

(f) whether Defendant's violations of BIPA were committed intentionally, recklessly, or negligently.

82. **Typicality and Adequate Representation**: Plaintiffs, who like other members of the putative class, had their biometrics captured and retained by Defendant, have claims that are typical of the class. Plaintiffs have retained and are represented by qualified and competent counsel who are highly experienced in complex privacy class action litigation. Plaintiffs and their counsel are committed to vigorously prosecuting this class action. Moreover, Plaintiffs are able to fairly and adequately represent and protect the interests of such a Class. Neither Plaintiffs nor their counsel have any interest adverse to, or in conflict with, the interests of the absent members of the Class. Plaintiffs have raised viable statutory claims of the type reasonably expected to be raised by members of the Class, and will vigorously pursue those claims. If necessary, Plaintiffs may seek leave of this Court to amend this Class Action Complaint to include additional Class representatives to represent the Class or additional claims as may be appropriate.

83. **Propriety of Class Treatment**: a class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of the claims of all Class members is impracticable. Even if every member of the Class could afford to invest the time and expense necessary to pursue individual litigation, the Court system could not. It would

be unduly burdensome to the courts in which individual litigation of numerous cases would proceed. Individualized litigation would also present the potential for varying, inconsistent or contradictory judgments, and would magnify the delay and expense to all parties and to the court system resulting from multiple trials of the same factual and legal issues. By contrast, the maintenance of this action as a class action presents few management difficulties, conserves the resources of the parties and of the court system and protects the rights of each member of the Class. Plaintiffs anticipate no difficulty in the management of this action as a class action. Class-wide relief is essential to compliance with BIPA.

CLAIMS FOR RELIEF

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

84. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

85. Defendant, Lytx, is a private entity as contemplated by BIPA.

86. Lytx provides cameras to trucking companies, installs or assists in the installation of its cameras in trucks, leases its surveillance software to trucking companies, provides servicing and analysis of data obtained from its cameras and software, and stores the data obtained from its cameras and software internally.

87. BIPA requires any private entity in possession of biometric identifiers or biometric information to develop a publicly available written policy, establishing both a retention schedule and guidelines for the permanent destruction of biometric identifiers and biometric information. BIPA requires the policy to comply with destruction timelines of either (i) when the initial purpose for which the collection of such identifiers or information has been satisfied or (ii) within three years of the individual's last interaction with the private entity, whichever occurs first. 740 ILCS

14/15(a)

88. Lytx does not have a publicly available written retention schedule or guidelines for the destruction of biometric data anywhere on its website or otherwise available for review by the public. In fact, Lytx's Privacy Policy *expressly* indicates it does not apply "to the extent [it] process[es] Personal Information in the role of a service provider on behalf of [its] clients." Further, it directs the reader to the respective client for information pertaining to privacy and disclaims any responsibility for the "privacy or data security practices of our clients, which may differ from those set forth in this Privacy Policy."

89. Lytx's Terms of Service and Privacy Policy are silent on the issue of biometric identifiers or biometric information.

90. On behalf of themselves and the Class, Plaintiffs seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs 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 from Defendant for each intentional and/or reckless violation of BIPA or, in the alternative, statutory damages of $1,000 from Defendant 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

91. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

92. Defendant, Lytx, is a private entity as contemplated by BIPA.

93. BIPA requires private entities 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:

A. informs the subject…in writing that a biometric identifier or biometric information is being collected or stored;

B. informsthe subject…in writing of the specific purpose and length of term for which a biometric identifieror biometric information is being collected, stored, and used; **and**

C. receives a written release executed by the subject of the biometric identifier or biometric information…"

740 ILCS 14/15(b)(emphasis added).

94. Defendant failed to comply with these BIPA mandates.

95. Defendant systematically and automatically captured, collected, obtained, used, stored and disseminated Plaintiffs' and Class members' biometrics without first obtaining the written release required by 740 ILCS 14/15.

96. Defendant never informed Plaintiffs and the Class in writing that their biometrics were being captured, collected, obtained, stored, used and disseminated, nor did Defendant inform Plaintiffs and the Class in writing of the specific purpose(s) and length of term for which their biometrics were being collected, stored, used and disseminated as required by 740 ILCS 14/15.

97. By collecting, storing, using and disseminating Plaintiffs' and Class members' biometrics as described herein, Defendant violated Plaintiffs' and Class members' rights to privacy in their biometrics as set forth in BIPA. *See* 740 ILCS 14/1, *et seq*.

98. On behalf of themselves and the Class, Plaintiffs seek: (1) declaratory relief; (2)

injunctive and equitable relief as is necessary to protect the interests of Plaintiffs 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 from Defendant for each intentional and/or reckless violation of BIPA or, in the alternative, statutory damages of $1,000 from Defendant for each negligent violation of BIPA; and (4) reasonable attorneys' fees and costs and other litigation expenses. *See* 740 ILCS 14/20.

COUNT III
VIOLATION OF 740 ILCS 14/15(c)
Selling, Leasing, Trading, or Otherwise Profiting From a Person's or a Customer's Biometrics.

99. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

100. Defendant, Lytx, is a private entity as contemplated by BIPA.

101. Lytx develops, manufactures, and markets products to transportation clients, such as its MV+AI technology which, in its continuous monitoring of the machine operators, collects biometric identifiers or biometric information.

102. Lytx uses the collection of biometrics to further its capacity to engineer products which utilize biometric technology, having stored 100 billion miles of driving data on its servers for analysis and development.

103. Lytx additionally uses its collection of biometrics to market and sell its current products and services to new clients, increasing its market share of the biometrics industry.

104. BIPA expressly prohibits a "private entity in possession of a biometric identifier or biometric information" from "sell[ing], leas[ing], trad[ing], or otherwise profit[ing] from a person's or a customer's biometric identifier or biometric information." 740 Ill. Comp. Stat. Ann. 14/15(c).

105. As detailed herein, Defendant clearly and deliberately profited from the collection

of Plaintiffs' and Class Members' biometrics either through the reduction of costs as a result of the collection, or the collection, analysis, and repackaging of the data for sale and development of additional technologies.

106. On behalf of themselves and the Class, Plaintiffs seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs 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, Plaintiffs, on behalf of themselves and the proposed Class, respectfully request that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiffs as representatives of the Class, and appointing their 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 Plaintiffs and the Class their reasonable attorneys' fees and costs and other litigation expenses;

F. Awarding Plaintiffs 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.

Dated: November 22, 2024

Respectfully submitted,

/s/ Randall K. Pulliam

Randall K. Pulliam

Randall K. Pulliam, (admitted *pro hac vice*)
rpulliam@cbplaw.com
Samuel R. Jackson (admitted *pro hac vice*)
sjackson@cbplaw.com
CARNEY BATES AND PULLIAM, PLLC
519 West 7th Street
Little Rock, AR 72201
Telephone: (501) 312-8500
Facsimile: (501) 312-8505

J. Dominick Larry
NICK LARRY LAW LLC
8 S. Michigan Ave., Suite 2600
Chicago, IL 60603
Telephone: 773.694.4669
Facsimile: 773.694.4691
nick@nicklarry.law

Attorneys for Plaintiffs and the Class

Jason L. Lichtman (admitted *pro hac vice*)
jlichtman@lchb.com
Sean A. Petterson (admitted *pro hac vice*)
spetterson@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN LLP
250 Hudson St., 8th Floor
New York, New York 10013
(212) 355-9500

Douglas M. Werman
dwerman@flsalaw.com
WERMAN SALAS P.C.
77 W. Washington Street, Suite 1402
Chicago, Illinois 60602
(312) 419-1008

David Fish
dfish@fishlawfirm.com
WORKPLACE LAW PARTNERS, P.C.
111 E. Wacker Dr., Suite 2300
Chicago, IL 60601
(312) 861-1800

Gary M. Klinger
gklinger@milberg.com
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street,
Suite 2100
Chicago, IL 60606
(866) 252-0878

Attorneys for Plaintiffs and the Class