

**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 identifiers² and biometric information³ (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 or 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 as 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 and use 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.

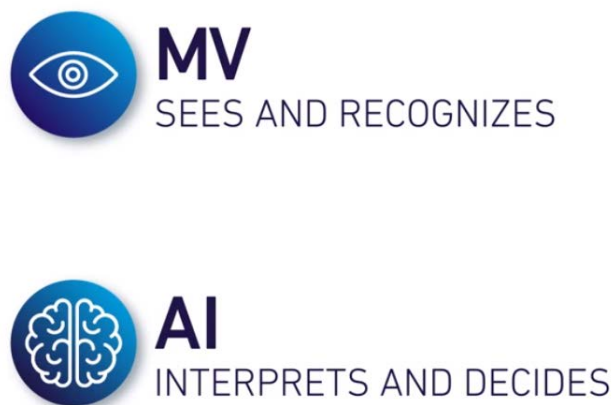
30. That algorithm is then deployed in the technology behind the DriveCam. The camera scans a driver’s face geometry, identifying a host of unique points around multiple regions of the driver’s face (*i.e.*, each eye, the mouth, the nose, the lips, etc.). Once the DriveCam has successfully detected a 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 2⁹

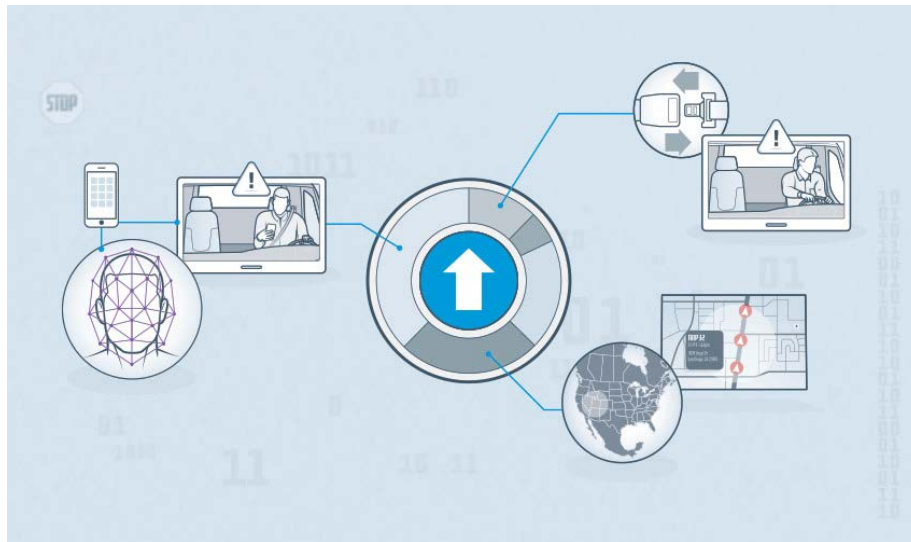


Figure 3¹⁰

⁹ <https://www.lytx.com/en-us/fleet-management/features/risk-id-without-recording> (attached as Exhibit 6)

¹⁰ Demystifying MV+AI, *supra*

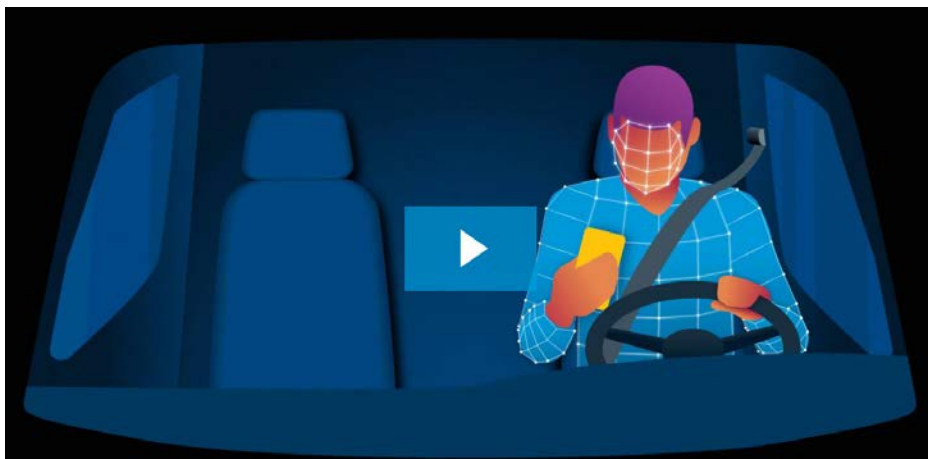


Figure 4¹¹

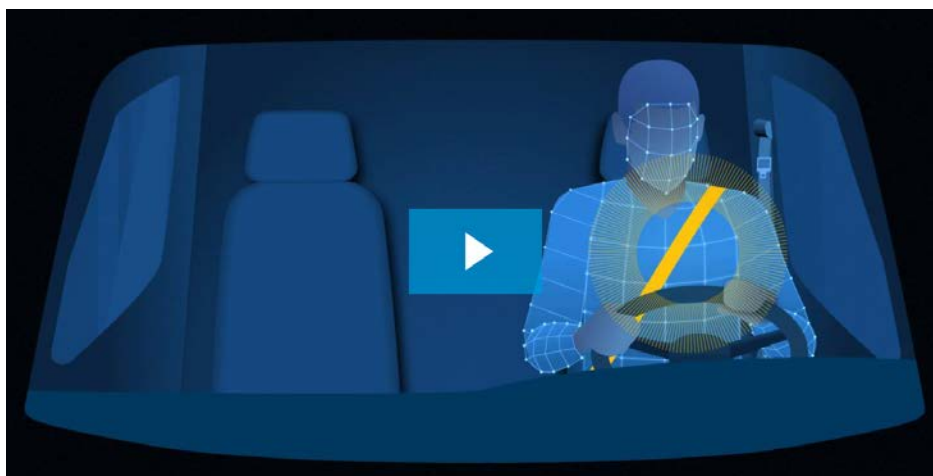


Figure 5¹²

¹¹ Our Technology, *supra*

¹² *Id.*



Figure 6¹³



Figure 7¹⁴

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.*

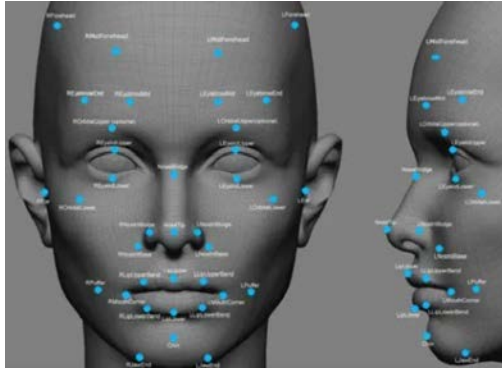


Figure 8¹⁹

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 9²¹

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 before capturing 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 before capturing 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 Approval³⁷ 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: January 20, 2025

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

One Allied Drive, Suite 1400

Little Rock, AR 72202

Telephone: (501) 312-8500

Facsimile: (501) 312-8505

J. Dominick Larry

NICK LARRY LAW LLC

1720 W. Division St.

Chicago, IL 60622

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

EXHIBIT 1

HARDWARE COMPARISON

LYTX[®] EVENT RECORDERS



SPECIFICATIONS	DC3P	ER-SV2	SF-SERIES
Event Recorder Unit			
Weight	.52 lb	.38 lb Base Unit: 2 lb 9 oz	.74 lb
Dimensions (W x H x D)	4.6 x 4.3 x 2.1 in 12 x 11 x 5 cm	4.6 x 3.2 x 2.3 in Base Unit: 8.5 x 5.0 x 1.5 in	5.0 x 4.2 x 2.2 in
Operating Temperature	-40°F to 185°F	-40°F to 185°F Base Unit: -40°F to 149°F	-40°F to 185°F
Microphone	Omnidirectional	Omnidirectional	Omnidirectional
In-Vehicle Audible Alerts on Select Triggers	No	No	SF300: Yes SF200: No SF64: No
Status Lights	2 LED (red, green)	7 LED (wide spectrum)	7 LED (wide spectrum)
Night Vision Illumination	6 high-lumen infrared LED lights	8 high-lumen infrared LED lights	8 high-lumen infrared LED lights
Manual Record Buttons	Yes	Yes	Yes
Industrial-grade Hardware	Yes	Yes	Yes
Limited Warranty	2 Years	2 Years	2 Years
Machine Vision + Artificial Intelligence (MV+AI)			
Configurable Inside View Triggers <ul style="list-style-type: none"> Handheld Device No Seat belt Driver Smoking Food or Drink 	No	No	SF300: All SF200: No SF64: No
Configurable Road View Triggers <ul style="list-style-type: none"> Rolling Stop Lane Departure Following Distance Critical Distance 	No	All	SF300: All SF200: Rolling Stop Only SF64: Rolling Stop Only
LytX Badge (Driver ID)	No	All	SF300: Yes SF200: Yes SF64: No
Internal			
Processor	Single-core 180 MHz	Quad-core 1 GHz	SF300: Dual Core 1.0 GHz; 512 KB cache SF200: Dual Core 1.0 GHz; 512 KB cache SF64: Dual Core 1.0 GHz; 512 KB cache
Internal Memory	128 MB	1 GB	SF300: 1 GB SF200: 1 GB SF64: 512 MB
Internal Storage	4 GB	16 GB	SF300: 16 GB SF200: 16 GB SF64: 64 GB
Memory Format	NAND	eMMC	eMMC
Expandable/External Memory	No	No	SF300: 128 GB SF200: 128 GB SF64: No

LYTX EVENT RECORDERS

SPECIFICATIONS	DC3P	ER-SV2	SF-SERIES
Internal (cont.)			
Motion Sensors	<ul style="list-style-type: none"> • 3-Axis (Accelerometer) • Built-in G-Force and motion sensor • Built-in GPS 	<ul style="list-style-type: none"> • 6-axis (Accelerometer + Gyro) • Built-in G-Force and motion sensor • Built-in GPS 	<ul style="list-style-type: none"> • 9-axis (Accelerometer + Gyro + Magnetometer) • Built-in G-Force and motion sensor • Built-in GPS
Recording			
Wide Angle Lens / Field of View	131° interior; 88° exterior	131° interior; 82° exterior	128° interior; 84° exterior (SF64) 128° interior; 78° exterior (SF200/SF300)
Video Recording Resolution	768 x 576	752 x 548	752 x 548 (SF64) 1280 x 800 (SF200/SF300)
Frame Rate	4 fps	10 fps	10 fps
DVR Capable	Yes	Yes	Yes
ActiveVision Capable	No	Yes	No Yes (SF300: MV+AI Road View)
ECM Support	<ul style="list-style-type: none"> • Speed Management • Fuel Reporting • ADAS Management 	<ul style="list-style-type: none"> • Speed Management • Fuel Reporting • ADAS Management • ActiveVision® Service/ Road View MV+AI 	<ul style="list-style-type: none"> • Speed Management • Fuel Reporting • ADAS Management • ActiveVision® Service/ Road View MV+AI
Configurable Internal / External Lens	Yes	No	Yes
Connectivity			
Cellular	CDMA or GSM	CDMA or GSM	CDMA or GSM
Wi-Fi via Hotspot	Wi-Fi b/g 2.4 GHz	Wi-Fi b/g/n 2.4 GHz	SF300: Wi-Fi b/g/n/ac 2.4/5 GHz SF200: Wi-Fi b/g/n/ac 2.4/5 GHz SF64: N/A
Bluetooth Capable	No	Yes	Yes
Ethernet	No	Yes	Yes
Power			
Battery	Non-rechargeable	Rechargeable	SF300: Rechargeable SF200: Rechargeable SF64: Non-rechargeable
Standard Input Voltage	12V or 24V	12V or 24V	12V or 24V
Power Draw (12V)			
Ignition On (cellular) • Not Transmitting • Transmitting	228mA	530mA	SF300: 320 mA SF200: 320 mA SF64: 228 mA
Ignition Off (cellular) • Not Transmitting • Transmitting	438 mA	620 mA	SF300: 540 mA SF200: 540 mA SF64: 438 mA
Power Draw (hibernation)	<1mA	<1mA	Hibernation: 20 mA (cellular on) Deep Sleep: <1 mA (cellular off)
Disconnect Reporting	Yes	Yes	Yes
Hibernation	Default: 15 Min	Default: 15 Min	Default: 15 Min
Installation			
Trigger In	Qty 2	Qty 5	Qty 4
Trigger Out	Qty 1	Qty 3	Qty 1
ECM / ECU Integration	Via VBI J1939 Via B&B module OBDII	J1939, FMS	J1939
Recommended Mounting Location	Windshield Bulkhead	Windshield Bulkhead	Windshield Bulkhead
Installation Services Available	Lytx Professional Installation Services Training & support for client-managed Installation	Lytx Professional Installation Services Training & support for client-managed Installation	Lytx Professional Installation Services Training & support for client-managed Installation

LYTX EVENT RECORDERS

SPECIFICATIONS	DC3P	ER-SV2	SF-SERIES
Included Accessories			
ECM Cable	No	Yes	Yes
Mounting Bracket	Non-removable	Non-removable Base Unit: Removable	Non-removable
Informational Guide	Yes	Yes	Yes

DISCLAIMER: Lytx® event recorders are intended as a driver aid only and are not a substitute for a safe, conscientious driver. Lytx event recorders cannot compensate for a driver that is distracted, inattentive, or impaired by fatigue, drugs, or alcohol. It is always the responsibility of the driver to take appropriate corrective action. Never wait for the Lytx event recorder to provide a warning before taking measures to avoid an accident. Failure to do so can result in serious personal injury or death, or severe property damage.

EXHIBIT 2

OUR STORY

Redefining safety on our roadways with innovation backed by experience

Industry-leading fleet and compliance management solutions

At Lytx®, we harness the power of video and data to enable fleets to improve safety, efficiency, and productivity. We're trusted by more than 4,000 fleets that log billions of miles worldwide each year, contributing to a vast and ever-growing database of driving data we use to refine the accuracy and effectiveness of our solutions. Our clients can realize significant returns on investment by lowering operating and insurance costs. Most of all, we strive to save lives—on our roads and in our communities, every day. We dream of a world where no commercial driver is ever the cause of a collision.

We're driven by a passion to improve safety on our roadways. Our solutions enhance vehicles with a suite of cloud-connected dash cams, sensors, [telematics](#), and services that help transform fleet safety and operations.



Our mission

We believe that video enriches everything. We empower optimal fleet visibility and operations through the power of video telematics.





Innovation guided by experience

We draw from more than 20 years of industry leadership to create smart solutions that truly help solve our customers' challenges. Our unparalleled database of driving behavior — more than 120 billion miles and growing each day — trains our machine vision and artificial intelligence-based solutions to recognize and flag risky driving with incredible accuracy. We cut through the noise to deliver real insights that help our clients save valuable time and prioritize focus where it matters most to help improve driver safety and protect their bottom lines.

[ABOUT OUR FLEET MANAGEMENT SOLUTIONS](#)

We're invested in your success

Our team offers customized support at every stage of the process, from trial to implementation, to ensuring return on investment.

[MEET OUR TEAM](#)



Improving safety on our roadways

Our passion for safety and saving lives drives incredible results.

1.3M

More than 1.3 million
drivers protected
worldwide

625K

Our clients saw 625,000
fewer instances of risky
driving in 2018*

120B

120 billion miles of
professionally analyzed
driving data

We've worked with companies across multiple industries with fleets from 5 to 500+ vehicles.

Industry

All

Fleet Size

All

Result

All

DISTRIBUTION

Murphy-Hoffman Company sees 79% reduction in roadway collisions with Lytx

79% reduction in on-roadway collisions
33% improvement in frequency and severity of incidents
59% reduction in cell phone usage while driving

Fleet Size: 500+

Result: Improve Driver Performance

TRUCKING

Dart Transit Company decreases near collisions by 65% with Lytx

65% decrease in near collisions
77% improvement in late response
69% improvement in following distance

Fleet Size: 500+

Result: Improve Driver Performance

GOVERNMENT

The City of Mobile, Alabama, reduces collisions by 62% with Lytx

62% reduction in collisions
39% reduction in risky driving behaviors
50% reduction in near collisions

Fleet Size: 50-499

Result: Manage Fleet Risk

DISTRIBUTION

Southern Maryland Oil reduces identified collisions by 59% with Lytx

86% reduction in cell phone use
69% improvement in unbelted events
59% reduction in identified* collisions

Fleet Size: 50-499

Result: Improve Driver Performance



TRUCKING

JBS Carriers sees an 80% improvement in traffic violations with Lytx

80% overall improvement in traffic violations
61% improvement in following distance
88% improvement in driver seat belt usage

Fleet Size: 500+

Result: Improve Driver Performance



GOVERNMENT

U.S. Department of State reduces near collisions with the Lytx Driver Safety Program

62% reduction in near collisions
54% decrease in the number of events
49% reduction in event severity

Fleet Size: 500+

Result: Improve Driver Performance



WASTE

Liquid Environmental Solutions reduces the severity of risky driving events with the Lytx Driver Safety Program

80% reduction in traffic violations
58% reduction in severity of risky driving events
61% reduction in cell phone use

Fleet Size: 50-499

Result: Manage Fleet Risk



TRUCKING

Cargo Transporters reduces fraudulent claims costs with the Lytx Driver Safety Program

83% decrease in near collisions
76% reduction in traffic violations
33% drop in unbelted drivers

Fleet Size: 500+

Result: Manage Fleet Risk

LOAD MORE

Industry involvement

Lytx is an active participant in 50 key industry associations that support and advocate for commercial transportation safety and the interests of our clients across the trucking, concrete, construction, waste, government, distribution, and field services industries. In addition, we participate in educational workshops, sponsor industry events, and support key initiatives. Our engagement at the industry level helps us stay abreast of trends, advocate for legislation, promote key market activities, and design solutions to address real-world challenges.

ABOUT WHO WE SERVE



More than 20 years of innovation

From monumental product launches to technological breakthroughs, here's a look in the rearview mirror at our history.



19
98

DriveCam, Inc. is founded

19
99

Introduced the first vehicle camera to record crashes

20
01

Developed a camera with both road-facing and driver-facing lens

20
02

Launched software to enable review and scoring of driving video

20
06

Introduced the driver coaching model

20
09

Launched online program management platform

20
11

Acquired RAIR Technologies® to round out compliance offering

20
13

Changed the company's name to Lytx, Inc.

20
15

Launched first camera equipped with machine vision and artificial intelligence

20
15

Launched continual video coverage and optional extra cameras

20
18

Surpassed 100 billion miles of driving data analyzed

20
19

Launched new, customizable fleet management solutions

Combine services to build a comprehensive solution that meets your needs



Driver safety solutions

Proactively manage your fleet risk with tools to help you change behavior, prevent collisions, and improve your bottom line.



Fleet tracking

Get real-time* access to fleet status to help you respond faster, reduce callbacks, and optimize productivity.



DOT compliance services

Meet the mandates with devices and services that streamline and simplify compliance management.

Subscribe to our newsletter

Our Best Fleet Forward newsletter delivers monthly insights on fleet management.

Get started today.

[1-866-419-5861](tel:1-866-419-5861) [Contact Us](#) [Book a Demo](#)

SOLUTIONS

[Fleet Management Overview](#)
[Fleet Dash Cams](#)
[Fleet Safety](#)
[Fleet Tracking](#)
[DOT Compliance](#)
[ELD Compliance](#)
[FedEx VEDR](#)
[Lytx Integration Network](#)

FEATURES

[DriveCam Event Recorder](#)
[Lytx Driver App](#)
[Machine Vision and Artificial Intelligence](#)
[Risk ID Without Recording](#)
[Continual Behavior Reporting](#)
[Preventative Maintenance](#)
[Diagnostic Trouble Codes](#)

SUPPORT & LOGIN

[Support](#)
[Lytx Account Login](#)
[Lytx Compliance Services \(RAIR\) Portal](#)
[Lytx DriveCam Academy](#)
[Parts Store](#)

GUIDES

[ADAS](#)
[CSA Scores](#)
[Defensive Driving for Commercial Fleets](#)
[Distracted Driving](#)
[DOT Regulations](#)
[ELD Guide](#)
[Fleet Maintenance](#)
[Fleet Management App](#)

ABOUT US

[Our Story](#)
[Our Technology](#)
[Our Team](#)
[Careers](#)
[News and Events](#)
[Who We Serve](#)
[Success Stories](#)

RESOURCES

[Blog](#)
[Buyer's Guide to Video Telematics](#)
[The Fleet Podcast](#)
[Videos](#)
[All Resources](#)

EXHIBIT 3

LYTX DRIVER SAFETY

Fleet safety solutions

Empower drivers to address distractions and avoid collisions with our configurable fleet safety program

Driver safety is key to protecting your bottom line

Start changing driver behavior today while also ensuring lasting change over the long haul. Our driver safety solutions help fleets achieve maximum, sustained results with minimal time and effort. Our driver-centric tools help you prevent collisions – before they happen – to protect your bottom line.

Our machine vision and artificial intelligence technology can help detect and deter distracted driving, adding a variety of flexible coaching options, customizable reporting, and accurate, professional review of more than 60 risky driving behaviors. It's a powerful, proven, and efficient solution to help improve fleet safety management and performance – quickly and easily.

[BOOK A DEMO](#)

□□□□□□□□

How it works

See what our fleet safety solutions can do for you.





Detect distracted driving in the moment with advanced MV+AI technology

Our [machine vision and artificial intelligence \(MV+AI\)](#) technology can help you detect distracted driving inside and outside the vehicle and alert your drivers to behaviors associated with collisions, including cell phone use, seat belt use, inattentiveness, eating and drinking, smoking, failure to stop at intersections, weaving within or departing from lanes, and unsafe following distances.

Not only that, you'll also have access to detailed reports that can track the duration of persistent behaviors and the percentage of drive time those behaviors consume. This can help you see how much time these habits are taking up your driver's day.

Accurate fleet safety insights you can trust

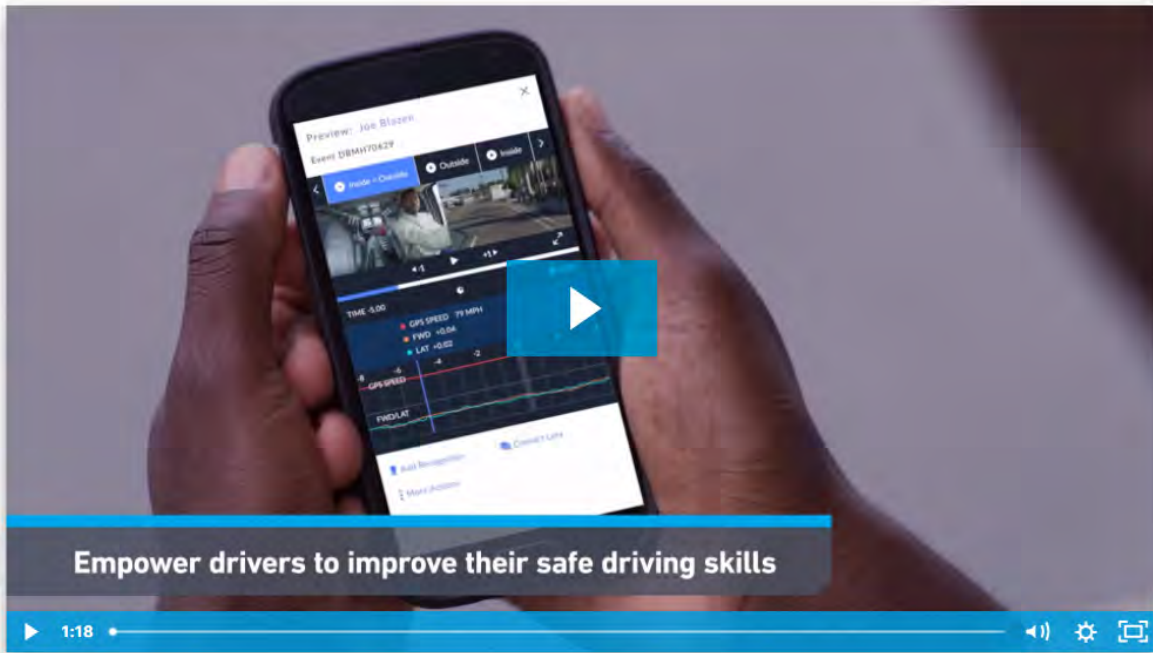
Lytx® MV+AI technology is informed by more than 20 years of commercial driving data — representing more than 120 billion miles from all types of vehicles and road conditions. This extensive database is made even more accurate through professional human review to validate and categorize driving behaviors. Accurate results save you the time and energy it takes to filter through notifications that don't represent true risk, while also helping to ensure you don't miss critical events.



Help drivers self-correct in the moment with real-time alerts

Real-time alerts[†] can help drivers redirect their attention in the moment to avoid potential collisions. Our alerts focus on the moments that matter, using MV+AI technology to focus on critical risks while avoiding the distraction and fatigue that can occur when alerts are overly frequent or inaccurate.

Our light and audio alerts can be configured to alert for when driving behaviors like inattentive driving, speeding, failure to wear a seat belt, smoking, eating or drinking, rolling stops, lane departures, forward collision potential, critical following distances, and using handheld devices occur. Drivers can review their own video and performance metrics after the drive and self-coach for continuous improvement.



AI RISK DETECTION

Identify unsafe driving behavior and prompt drivers with in-cab alerts[†] to help them self-correct in the moment.

REMOTE COACHING

Help drivers improve, even when face-to-face meetings aren't possible, with a remote coaching workflow.

DRIVER SAFETY INSIGHTS

Analyze driving performance and trends to help improve safety and efficiency across your fleet.

POSITIVE DRIVER RECOGNITION

Empower and recognize your drivers to reinforce safe driving behavior and improve overall fleet safety.

[BOOK A DEMO](#)

Manage driver safety without recording video of the driver

You can configure the Lytx MV+AI technology to actively monitor the driver's patterns of movement and capture unwanted or distracted behaviors in the form of metadata — [without recording video of the driver](#). This innovative lens configuration option gives fleet managers the power to manage distractions without recording the inside view of the vehicle, which can be key to a safer fleet.

[EXPLORE RISK ID WITHOUT RECORDING](#)



Configurable coaching options to meet your business needs



Most professional drivers are capable of self-correcting in the moment. But for those who need more help, Lytx offers a range of tools that help drive long-term behavior change across your spectrum of risk. Our proven video-based coaching workflows can be used as needed to support:

- Traditional, face-to-face coaching sessions
- Remote coaching to support drivers when in-person sessions aren't practical
- Self-coaching that empowers drivers to learn and improve on their own
- Performance review after the drive through an engaging [fleet driver app](#) that allow drivers to see moments of risk first-hand and optimize future behavior

Analyze your results with comprehensive reporting

Get comprehensive, customizable reporting on your fleet safety program, from industry benchmarks to progress against internal metrics to ROI analysis. You'll have the full picture so you can see the real results of your investment, prove the fleet safety program's effectiveness, and ensure ongoing executive support.

Coaches by Lowest Effectiveness					View Details	
Last 90 Days						
COACH	COACHING EFFECTIVENESS	AVG DAYS TO COACH	COACHED EVENTS	WITH NOTES		
David Lytx	Behaviors by Highest Frequency	29.3	3	100.0%		
Aaron Howell	Left Yth Drive	0.0	0	0.0%		
AJ Strazzeri	RECOVER	0.0	538	0.0%	TREND	
Alberto Valls	Posted Speed Violation	0.0	0	0.0%	▲ 120%	
Alex Black	Speed Policy Violation	0.0	312	0.0%	▲ 51%	
	Following Distance - 2 seconds		46		▲ 283%	
	Following Distance - 3 seconds		21		0%	
	Following Distance - 4 seconds		10		▲ 100%	

Compare safety solutions

Other driver safety solutions

Driver safety features offered by other vendors.

Lytx driver safety solutions

Lytx combines innovation and experience to deliver the most accurate risk insights available.

REAL-TIME, IN-CAB ALERTS†

Allow drivers to self-correct risky driving in the moment.



PROGRESS REPORTS

Risk reports help you track progress toward safety metrics and achieve accountability.



CONFIGURABLE DASH CAM VIEWS

Capture in-vehicle and road views with support for auxiliary cameras to add side and rear views.



DRIVER APP

Engage drivers after the trip and allow them to observe their performance to optimize future trips.



INTELLIGENT DASH CAM TECHNOLOGY

Get insights and detect risk with devices powered by advanced machine vision and artificial intelligence.



TECHNOLOGY BACKED BY DATA

Count on accurate insights powered by the world's largest commercial driving database of its kind.



ON-DEMAND* ACCESS TO VIDEO

Immediately access the video you need within minutes of capture.



PROACTIVE DISTRACTED DRIVING DETECTION

Accurately identify distracted driving behavior including cell phone use and inattentive driving.



IDENTIFY RISK WITHOUT RECORDING

Manage driving safety in real time without recording video of the driver.



"Since activating the machine vision and artificial intelligence capabilities within the Lytx Driver Safety Program, we're seeing a fuller, more accurate picture of risk in our fleet. We're able to bring our drivers' attention to risky habits in real time and offer coaching sessions as needed."

Patrick Landreth, Vice President of Safety and Human Resources, Ozark Motor Lines

Powered by the innovative Lytx DriveCam device

Machine vision and artificial intelligence (MV+AI) combine to deliver real-time alerts[†] that can help address distracted driving in the moment, and provide reliable, continual video evidence for protection when the unexpected occurs.



REAL-TIME, IN-CAB ALERTS[†]

Light and audio alerts notify drivers of their risky behaviors, helping them stay focused on the road (audio alerts available on SF300 only)



CONTINUAL VIDEO

Records up to 100 hours of reliable, continual video



INTEGRATED MV+AI

Advanced Machine Vision and Artificial Intelligence capture and accurately categorize risky driving behaviors



RISK DETECTION WITHOUT RECORDING

Manage distracted driving and other unwanted behaviors without recording video of the driver



LIVE STREAMING

See what's happening in and around vehicles in near real time



MANUAL RECORD BUTTONS

Enables your drivers to proactively record video when needed

[SEE ALL CAMERA SPECS](#)

Frequently asked questions

What are the benefits of a fleet safety program?



How does a fleet safety program work?



How does coaching help change driver behavior?



How do I review risky driving data?



Does my company need a fleet safety program?



Do I need to know how to get fleet safety certified?



We help deliver safety, success, and peace of mind for customers just like you.

Lytx® protects fleets from 5 to 500+ vehicles across multiple industries. Learn more about how we're helping to improve safety at companies like yours.

Industry

All industries



DISTRIBUTION

Murphy-Hoffman Company sees 79% reduction in roadway collisions with Lytx

79% reduction in on-roadway collisions
33% improvement in frequency and severity of incidents
59% reduction in cell phone usage while driving

Fleet Size: 500+

Result: Improve Driver Performance



TRUCKING

Dart Transit Company decreases near collisions by 65% with Lytx

65% decrease in near collisions
77% improvement in late response
69% improvement in following distance

Fleet Size: 500+

Result: Improve Driver Performance

Combine services to build a comprehensive solution that meets your needs



Fleet dash cams

Capture critical incidents with cloud-connected, continually recorded video and find the clips you need to understand what really happened within minutes.*



Fleet tracking

Get real-time* access to fleet status to help you respond faster, reduce callbacks, and optimize productivity.



DOT compliance services

Meet the mandates with devices and services that streamline and simplify compliance management.

Investing in video can lead to significant savings

Learn more about our pricing and how an investment today can result in years of savings.

[CALCULATE YOUR SAVINGS](#)

RELATED RESOURCES

Let technology do the heavy lifting to help ensure safer driving across your fleet.

Learn more about how our driver safety solutions can support your business and your drivers.

[All Resources](#)



ACCELERATING FLEET SAFETY FOR 2020 AND BEYOND

Learn about trending driving behaviors—what they are and how to identify them in our recent webinar with EHS.

[Read now](#)



HOW DURHAM COCA-COLA BOTTLING CO. ENSURES SAFETY WITH VIDEO TELEMATICS

Find out how Durham Coca-Cola Bottling Co. exonerated a driver from a false claim and reduced its claims cost by 92 percent using video telematics.

[Read now](#)



FUELING A SUCCESSFUL SAFETY CULTURE

Safety leaders across several industries share how they managed to get organization-wide support on safety.

[Read now](#)

THE LYTX DIFFERENCE



Service

Our team is invested in your success. We work with you to help ensure that your company achieves extraordinary results, from configuring the right solutions to meet your business needs to helping you get the greatest return on your investment. We're always expanding by listening to our customers and



Innovation

Our machine vision and artificial intelligence are powered by a robust driving database (120 billion miles and counting), resulting in connected, accurate, actionable insights that keep fleets safe, on-schedule, efficient, and productive. We continuously evolve to deliver cutting-edge updates that help customers



Leadership

For more than 20 years, Lytx has been a leading provider of complete fleet management solutions. We're focused on addressing all of your fleet needs, all in one place, with all together powerful solutions. We help fleets identify risk, stay safer, optimize efficiency and gain greater productivity. Our smart, simple hardware,

using their input to shape our next generation of features and capabilities.

simplify processes, save time, and focus on driving results for their business.

software, and API integrations provide a single, consolidated view of your fleet.

Subscribe to our newsletter

Our Best Fleet Forward newsletter delivers monthly insights on fleet management.

Get started today.

[1-866-419-5861](tel:1-866-419-5861) [Contact Us](#) [Book a Demo](#)

SOLUTIONS

- [Fleet Management Overview](#)
- [Fleet Dash Cams](#)
- [Fleet Safety](#)
- [Fleet Tracking](#)
- [DOT Compliance](#)
- [ELD Compliance](#)
- [FedEx VEDR](#)
- [Lytx Integration Network](#)

GUIDES

- [ADAS](#)
- [CSA Scores](#)
- [Defensive Driving for Commercial Fleets](#)

FEATURES

- [DriveCam Event Recorder](#)
- [Lytx Driver App](#)
- [Machine Vision and Artificial Intelligence](#)
- [Risk ID Without Recording](#)
- [Continual Behavior Reporting](#)
- [Preventative Maintenance](#)
- [Diagnostic Trouble Codes](#)

ABOUT US

- [Our Story](#)
- [Our Technology](#)
- [Our Team](#)
- [Careers](#)

SUPPORT & LOGIN

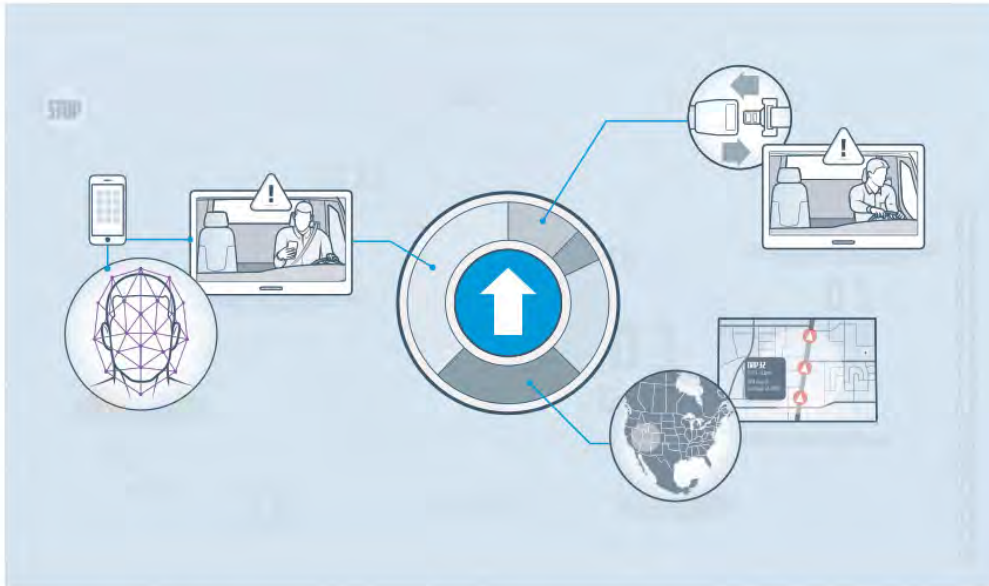
- [Support](#)
- [Lytx Account Login](#)
- [Lytx Compliance Services \(RAIR\) Portal](#)
- [Lytx DriveCam Academy](#)
- [Parts Store](#)

RESOURCES

- [Blog](#)
- [Buyer's Guide to Video Telematics](#)
- [The Fleet Podcast](#)
- [Videos](#)

EXHIBIT 4

Demystifying MV+AI Technology



What are Machine Vision and Artificial Intelligence (MV+AI)?

Machine Vision (MV) is a suite of sensor technologies that work together to recognize objects and behavior using visual data. Artificial intelligence (AI) enables computers to recognize patterns and make informed predictions about what might happen next. Together, these technologies can detect environments, discover which patterns correlate with risk, and determine potential outcomes.

MV+AI can recognize when a driver is distracted – by a mobile phone, for example – and prompt the driver with an alert before something potentially goes wrong. This is made possible by a comprehensive “training” process: hundreds of thousands of images feed the technology to teach the MV algorithm what distracted driving, and other behaviors look like. This training data is combined with additional information from GPS and a multitude of other sensors to teach the AI how to reliably detect more complex location-based behavior.

Still, the algorithms can't learn in a vacuum: human judgement plays a vital role in helping the system learn to spot driving conditions and driver behavior. Video is reviewed and the images are tagged to train the AI in knowing which data to consider more relevant. As the MV+AI system continues to learn, it identifies the correlation between behavior and risk more precisely, helping fleet managers identify which behaviors, locations, and drivers pose the greatest potential danger. In this way, MV+AI provide visibility into issues that were impossible to see just a few years ago.

MV+AI: An Extra Pair of Eyes

The combination of machine (MV) and artificial intelligence (AI) brings the promise of detecting and anticipating risk, helping drivers avoid collisions and making the world safer. This technology serves as a tireless pair of extra eyes that can help alert drivers to hazards – including their own bad habits – and drive more safely.

But not all MV+AI systems are created equally. Without large amounts of high quality data, even the best algorithms can't know what to look for. As advanced as machine learning has become, it still requires both billions of data points and expert humans to help train the technology to detect risk.

What Makes Lytx So Precise?

The MV+AI model is only as smart as the data used to train it. That's why it is important for humans to help: the system can't become an expert without the help of people who know which data is significant and what can be safely ignored.

Today, Lytx MV+AI technology focuses specifically on the challenges of detecting risk in commercial fleets. Our technology draws from a cache of images collected over 100 billion miles of driving, tagging them for potentially hazardous behaviors and conditions. This combination of human analysis with traditional [telematics data](#) provides more insight than machine analysis of raw data alone.

Expanded View Of Risk?

Lytx uses innovative technology to reliably uncover true risk so you can focus on what matters without the distraction of irrelevant events or information. Our focus on training algorithms with the best data provides the most precise results possible, avoiding the false positives that come from subpar or un-curated data.

Our technology is developed with one purpose in mind: delivering a view of fleet risk you can trust. 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.

Learn more about Lytx's [fleet safety](#) and [fleet tracking](#) solutions, and the [DriveCam](#) device that powers it all. [Schedule a free demo.](#)

Subscribe to the
Lytx blog for the
latest in fleet
management.

Work Email

NEXT RECOMMENDATION



What is a CMV? Commercial Motor Vehicle Definition

What is a CMV (Commercial Motor Vehicle) From what is considered a CMV to requirements for a CMV driver, we...



Subscribe to our newsletter

Our Best Fleet Forward newsletter delivers monthly insights on fleet management.

First name

Last name

Email address

SUBMIT

Get started today.

[1-866-419-5861](#) [Contact Us](#) [Book a Demo](#)

SOLUTIONS

[Fleet Management Overview](#)
[Fleet Dash Cams](#)
[Fleet Safety](#)
[Fleet Tracking](#)
[DOT Compliance](#)
[ELD Compliance](#)
[FedEx VEDR](#)
[Lytx Integration Network](#)

FEATURES

[DriveCam Event Recorder](#)
[Lytx Driver App](#)
[Machine Vision and Artificial Intelligence](#)
[Risk ID Without Recording](#)
[Continual Behavior Reporting](#)
[Preventative Maintenance](#)
[Diagnostic Trouble Codes](#)

SUPPORT & LOGIN

[Support](#)
[Lytx Account Login](#)
[Lytx Compliance Services \(RAIR\) Portal](#)
[Lytx DriveCam Academy](#)
[Parts Store](#)

GUIDES

[ADAS](#)
[CSA Scores](#)

ABOUT US

[Our Story](#)
[Our Technology](#)

RESOURCES

[Blog](#)
[The Fleet Business](#)

#1181

Defensive Driving for Commercial
Fleets
Solutions to Texting and Driving
Distracted Driving
DOT Regulations
Fleet Management Solutions
Fleet Risk Management
Fuel Management Systems
Telematics Systems

Our Team
Careers
News and Events
Who We Serve
Success Stories

Videos
All Resources

SITES

English (U.S.A.)
English (U.K.)



WARNING — The Lytx Event Recorder is a driver aid only. Never wait for the device to provide a warning before taking measures to avoid an accident.
Limited time offer. Trial services are provided at no cost for up to 1 month. Fees for shipment of hardware may apply.
* Subject to available cellular network coverage.
* Estimate based upon select sampling of Lytx client data.
© Copyright Lytx, Inc. 2021. All rights reserved.

[Site Map](#) [Legal](#) [Terms](#) [Privacy](#) [Driver Info](#)



EXHIBIT 5

OUR TECHNOLOGY

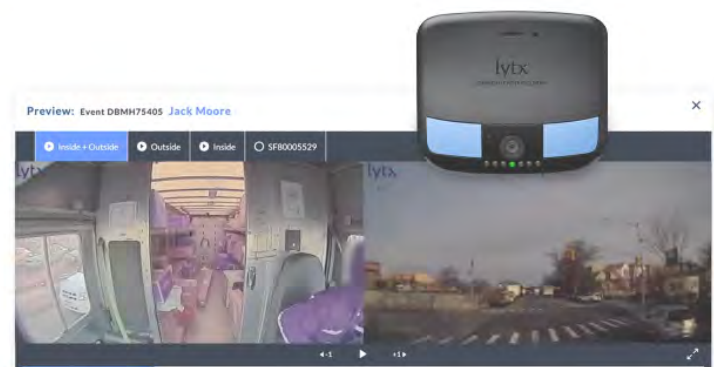
Machine vision + artificial intelligence

Award-winning technology helps detect and deter risky and distracted driving in real time

Addressing distracted driving — one of the biggest issues facing our roads today

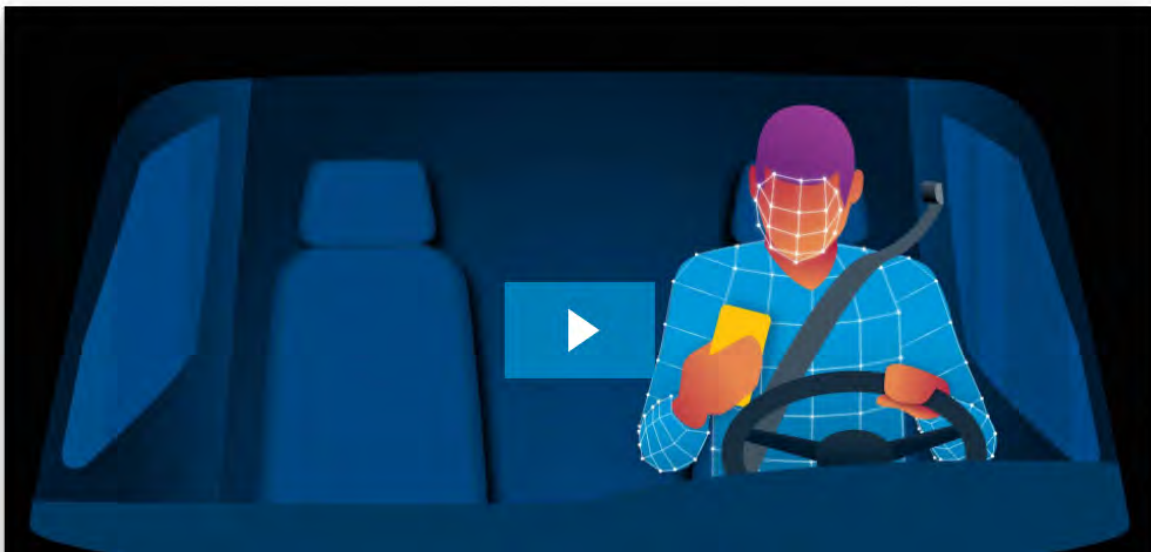
Lytx has expanded its machine vision system and artificial intelligence (MV+AI) technology on all [dash cam devices](#) to help drivers and fleet managers correct distracted driving as it occurs. Our unique machine vision technology helps identify distraction and risk, both inside and outside of the vehicle, including cell phone use, eating or drinking, smoking, seat belt use, general inattentiveness, failure to stop at intersections, weaving within or departing from lanes, and unsafe following distances.

MV+AI can provide in-cab alerts[†] that help empower drivers to change behavior in real time to avoid potential collisions. A complementary Lytx app helps your driver review their performance, self-coach, and optimize their driving for the next trip. Video footage and comprehensive dashboards help fleet managers track progress, drive accountability, and offer additional coaching, if needed.

[BOOK A DEMO](#)

Identify distracted and risky driving behavior inside the vehicle

MV+AI works to help identify the hard-to-detect distractions that drivers face today.



CELL PHONES AND HANDHELD DEVICES

Despite laws restricting cell phone use, they consistently remain involved in fatal collisions. MV+AI can detect unsafe cell phone use with a high degree of confidence, then it can deliver a timely in-cab alert to help drivers regain focus.

SEAT BELT USE

Seat belts save more than 15,000 lives each year. MV+AI can help identify and notify unbelted drivers so they can address the issue right away.

EATING AND DRINKING

Eating and drinking can cause a variety of distractions for drivers and issues with messy vehicles. In-cab alerts and video evidence help pinpoint when eating or drinking is potentially risky.

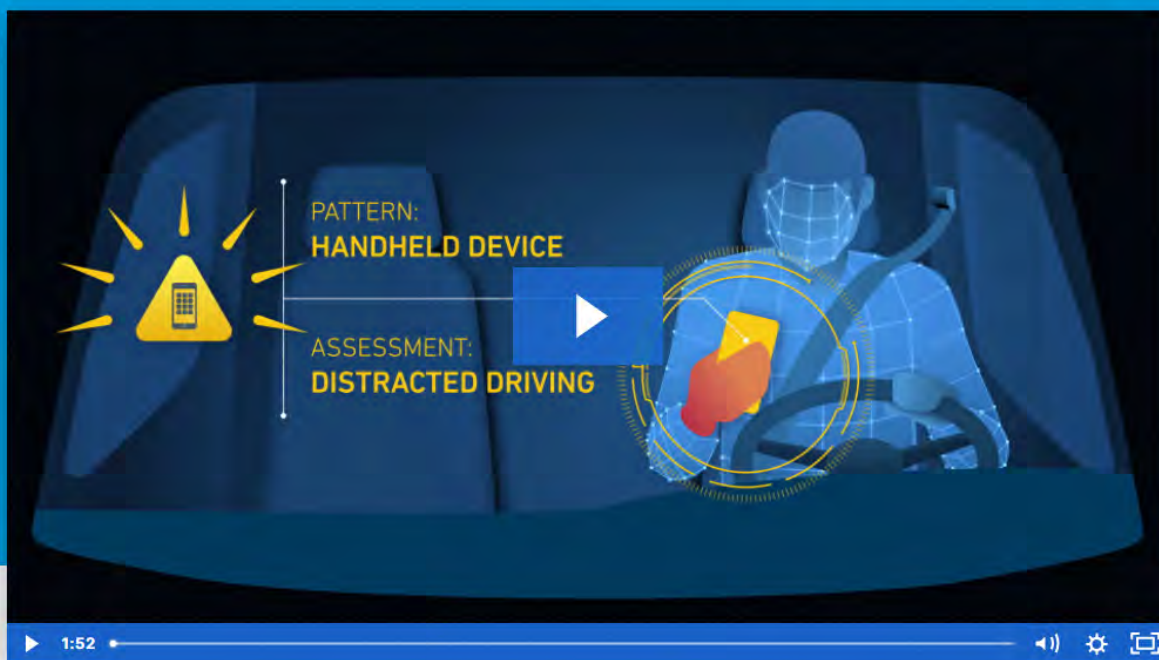
SMOKING

Smoking takes a driver's hands off the wheel and eyes off the road, and can pose risks around fuel or hazardous materials. MV+AI can detect smoking and alert drivers to stop.



How it works

See how machine vision and artificial intelligence work together to recognize and help stop risky driving in its tracks



Machine vision systems and artificial intelligence detect distraction and risk

Lytix MV+AI technology is constantly working to scan and evaluate driving patterns to determine potential risk. Machine vision operates as our system's eyes, allowing the technology to see and recognize objects. Artificial Intelligence is like the brain providing the system's ability to interpret and decide. For example, machine vision sees a cell phone in a vehicle, whether it is on the passenger seat or held to the driver's ear. Artificial intelligence then interprets cell phone images and recognizes that the phone on the seat does not represent risk, but the phone in the driver's hand does.

Identify additional risk on the road

In addition to our new, in-vehicle capabilities, Lytx has been applying MV+AI technology to detect risk on the road ahead for many years. MV+AI can reliably detect and record road-facing risk, including:

- Failure to stop at intersections
- Weaving within or departing from lanes
- Unsafe following distances



Our data helps MV+AI deliver accurate insights

To be effective, MV+AI algorithms must be highly accurate. Too many false alarms and drivers will ignore alerts. False negatives lead to missing critical events. Lytx MV+AI is backed by a peerless database of commercial driving behaviors, representing more than 120 billion miles driven in all types of vehicles and road conditions—validated by professional analysts. This allows our MV+AI solutions to identify driving behaviors with high levels of accuracy so drivers and fleet managers only get notified about the moments that matter.

Configurable coaching options support drivers

Lytx MV+AI integrated dash cams can capture moments of risky and distracted driving, delivering [in-cab alerts](#) that allow drivers to address risk in the moment, and video for review through an app to optimize their performance for the next trip. Fleet managers can use video and comprehensive dashboards and reporting to track progress, drive accountability and provide coaching, if needed.



Frequently asked questions

What is machine vision?



What is artificial intelligence?



How can I get the new MV+AI distracted driving features for my fleet?



What Lytx products include MV+AI technology?



How are risky or distracted driving insights delivered?



Combine services to build a comprehensive solution that meets your needs



Driver safety solutions

Proactively manage your fleet risk with tools to help you change behavior, prevent collisions, and improve your bottom line.



Fleet tracking

Get real-time* access to fleet status to help you respond faster, reduce callbacks, and optimize productivity.



DOT compliance services

Meet the mandates with devices and services that streamline and simplify compliance management.

Subscribe to our newsletter

Our Best Fleet Forward newsletter delivers monthly insights on fleet management.

SUBMIT

Get started today.

[1-866-419-5861](tel:1-866-419-5861) [Contact Us](#) [Book a Demo](#)

SOLUTIONS

- [Fleet Management Overview](#)
- [Fleet Dash Cams](#)
- [Fleet Safety](#)
- [Fleet Tracking](#)
- [DOT Compliance](#)
- [ELD Compliance](#)
- [FedEx VEDR](#)
- [Lytx Integration Network](#)

GUIDES

- [ADAS](#)
- [CSA Scores](#)
- [Defensive Driving for Commercial Fleets](#)
- [Distracted Driving](#)
- [DOT Regulations](#)

FEATURES

- [DriveCam Event Recorder](#)
- [Lytx Driver App](#)
- [Machine Vision and Artificial Intelligence](#)
- [Risk ID Without Recording](#)
- [Continual Behavior Reporting](#)
- [Preventative Maintenance](#)
- [Diagnostic Trouble Codes](#)

ABOUT US

- [Our Story](#)
- [Our Technology](#)
- [Our Team](#)
- [Careers](#)
- [News and Events](#)
- [Who We Serve](#)

SUPPORT & LOGIN

- [Support](#)
- [Lytx Account Login](#)
- [Lytx Compliance Services \(RAIR\) Portal](#)
- [Lytx DriveCam Academy](#)
- [Parts Store](#)

RESOURCES

- [Blog](#)
- [Buyer's Guide to Video Telematics](#)
- [The Fleet Podcast](#)
- [Videos](#)
- [All Resources](#)

#1187

ELD Guide

Fleet Maintenance

Fleet Management App

Fleet Management Solutions

Fleet Risk Management

Fuel Management Systems

Solutions to Texting and Driving

Telematics Systems

Success Stories

SITES

English (U.S.A.)

EXHIBIT 6

LYTX FEATURES

Lytix Risk ID Without Recording

Manage risky behavior without recording the driver

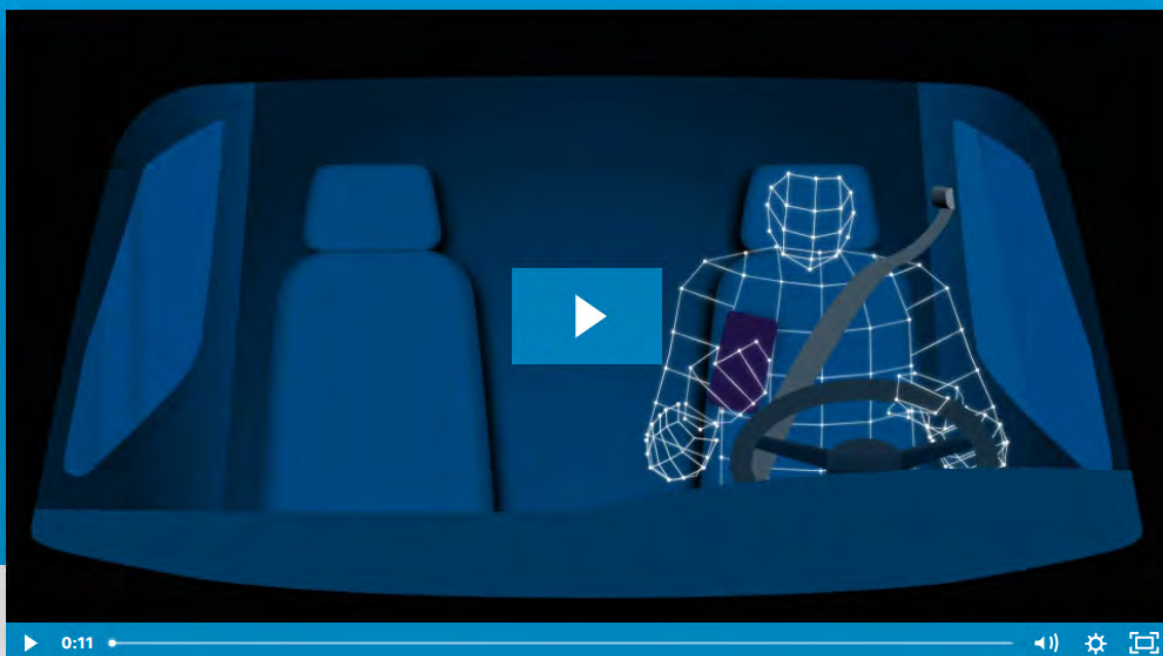
Capture risky driving without recording in-cab video

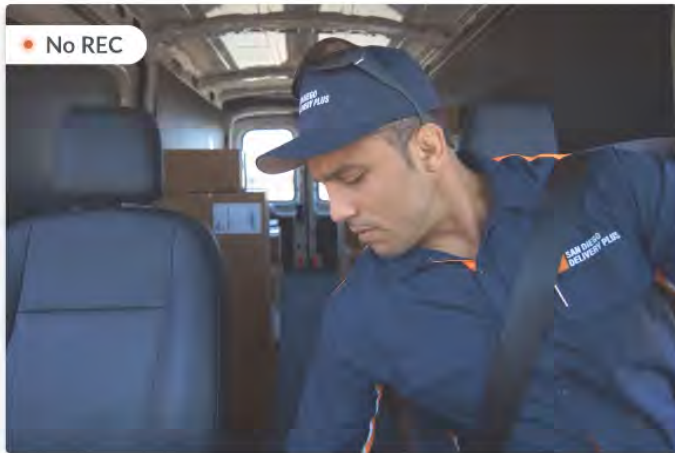
Lytix® Risk ID Without Recording helps you protect your fleet against distracted driving with a configurable option that allows fleet managers to take advantage of AI-powered risk detection without recording the inside view of the vehicle. It is part of Lytx's set of driver-centric tools that can help improve fleet safety management and performance – quickly, efficiently, and easily.

BOOK A DEMO



How it works





Detect and manage distracted driving

Managing distractions is critical to safe fleet operation, but there are situations that might call for different camera lens configuration options. Using Lytx's ultra-precise machine vision and artificial intelligence (MV+AI), the DriveCam Event Recorder can detect patterns of distracted or unwanted driving behaviors inside the cab without recording video of the driver. This enables the proactive capture of designated in-cab driving behaviors -- using a handheld device, improper seat belt use, inattentive driving, smoking, or eating and drinking -- without having inside-lens footage stored on the device.

Tapping into MV+AI and 120 billion of miles of data

Lytx's mature [MV+AI technology](#), vast data set, and algorithms refined with human input give our distracted driving detection a level of accuracy that allows us to capture distracted behaviors without using video. This is possible because Lytx MV+AI technology actively monitors the driver's patterns of movement, capturing unwanted and distracted behaviors in the form of metadata rather than video.

BEHAVIOR	DURATION	% OF DRIVE TIME
Driver Smoking	1m 10s	0.02%
Food or Drink	41m 12s	0.87%
Handheld Device	2h 15m 40s	2.21%
Inattentive	3m 40s	0.13%

See how much time risky behavior is consuming

Duration reporting can help managers understand the extent of a problem by calculating the percentage of trip time (ignition on to ignition off) that the driver was distracted. Lytx's MV+AI technology compiles this data and delivers it to your Lytx account without recording or saving inside-view video to the device.

Enable real-time, in-vehicle alerts for drivers

Even without video to help correct driving behavior, drivers can benefit from Lytx's real-time[†] alerts. These audio alerts are based on [risky](#) behaviors that are detected, but not recorded, enabling in-the-moment correction for greater overall safety. Risk ID Without Recording gives fleet managers the option to enable in-vehicle alerts, without recording or storing video.



READ NEXT

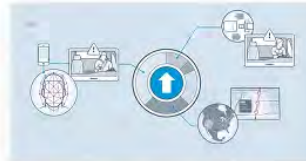
See the technology behind Risk ID Without Recording



LYTX DRIVECAM: INTELLIGENT DASH CAM TECHNOLOGY

Get the details about the DriveCam® Event Recorder, a 2020 EC&M Product of the Year award winner.

[Learn more](#)



DEMYSTIFYING MV+AI TECHNOLOGY

See how Lytx uses large volumes of high-quality data to give you the most accurate picture of your fleet's risk.

[Read now](#)



LYTX DRIVER SAFETY SOLUTIONS

See how Lytx can develop a comprehensive view of your driver's risk on the road.

[Read now](#)

Subscribe to our newsletter

Our Best Fleet Forward newsletter delivers monthly insights on fleet management.

First name

Last name

Email address

Get started today.

1-866-419-5861

[Contact Us](#)

[Book a Demo](#)

SOLUTIONS

[Fleet Management Overview](#)
[Fleet Dash Cams](#)
[Fleet Safety](#)
[Fleet Tracking](#)
[DOT Compliance](#)
[ELD Compliance](#)
[FedEx VEDR](#)
[Lytx Integration Network](#)

FEATURES

[DriveCam Event Recorder](#)
[Lytx Driver App](#)
[Machine Vision and Artificial Intelligence](#)
[Risk ID Without Recording](#)
[Continual Behavior Reporting](#)
[Preventative Maintenance](#)
[Diagnostic Trouble Codes](#)

SUPPORT & LOGIN

[Support](#)
[Lytx Account Login](#)
[Lytx Compliance Services \(RAIR\) Portal](#)
[Lytx DriveCam Academy](#)
[Parts Store](#)

EXHIBIT 7



Follow

595K Followers

Editors' Picks

Features

Deep Dives

Grow

Contribute

About

Face Detection For Beginners



Divyansh Dwivedi · Apr 27, 2018 · 7 min read



Multiple face detection in an image

In the past few years, face recognition owned significant consideration and appreciated as one of the most promising applications in the field of image analysis. Face detection can consider a substantial part of face recognition operations. According to its strength to focus computational resources on the section of an image holding a face. The method of face detection in pictures is complicated because of variability present across human faces such as pose, expression, position and orientation, skin colour, the presence of glasses or facial hair, differences in camera gain, lighting conditions, and image resolution.

Object detection is one of the computer technologies, which connected to the image processing and computer vision and it interacts with detecting instances of an object such as human faces, building, tree, car, etc. The primary aim of face detection algorithms is to determine whether there is any face in an image or not.

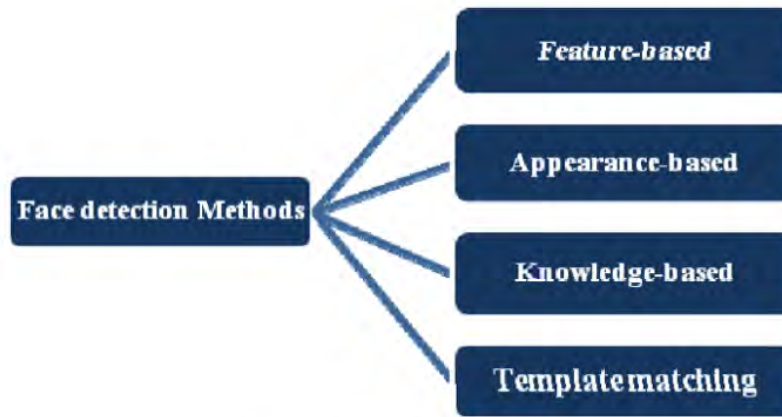
In recent times, a lot of study work proposed in the field of Face Recognition and Face Detection to make it more advanced and accurate, but it makes a revolution in this field when Viola-Jones comes with its Real-Time Face Detector, which is capable of detecting the faces in real-time with high accuracy.

Face Detection is the first and essential step for face recognition, and it is used to detect faces in the images. It is a part of object detection and can use in many areas such as security, bio-metrics, law enforcement, entertainment, personal safety, etc.

It is used to detect faces in real time for surveillance and tracking of person or objects. It is widely used in cameras to identify multiple appearances in the frame Ex- Mobile cameras and DSLR's. Facebook is also using face detection algorithm to detect faces in the images and recognise them.

Face Detection Methods:-

Yan, Kriegman, and Ahuja presented a classification for face detection methods. These methods divided into four categories, and the face detection algorithms could belong to two or more groups. These categories are as follows-



Different types of Face Detection Methods

1.Knowledge-Based:-

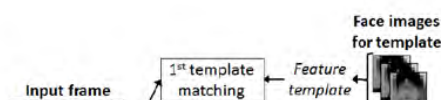
The knowledge-based method depends on the set of rules, and it is based on human knowledge to detect the faces. Ex- A face must have a nose, eyes, and mouth within certain distances and positions with each other. The big problem with these methods is the difficulty in building an appropriate set of rules. There could be many false positive if the rules were too general or too detailed. This approach alone is insufficient and unable to find many faces in multiple images.

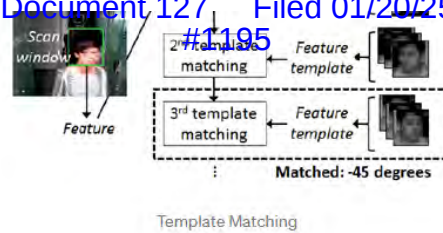
2.Feature-Based:-

The feature-based method is to locate faces by extracting structural features of the face. It is first trained as a classifier and then used to differentiate between facial and non-facial regions. The idea is to overcome the limits of our instinctive knowledge of faces. This approach divided into several steps and even photos with many faces they report a success rate of 94%.

3.Template Matching:-

Template Matching method uses pre-defined or parameterised face templates to locate or detect the faces by the correlation between the templates and input images. Ex- a human face can be divided into eyes, face contour, nose, and mouth. Also, a face model can be built by edges just by using edge detection method. This approach is simple to implement, but it is inadequate for face detection. However, deformable templates have been proposed to deal with these problems.





4.Appearance-Based:-

The appearance-based method depends on a set of delegate training face images to find out face models. The appearance-based approach is better than other ways of performance. In general appearance-based method rely on techniques from statistical analysis and machine learning to find the relevant characteristics of face images. This method also used in feature extraction for face recognition.

The appearance-based model further divided into sub-methods for the use of face detection which are as follows-

4.1.Eigenface-Based:-

Eigenface based algorithm used for Face Recognition, and it is a method for efficiently representing faces using Principal Component Analysis.

4.2.Distribution-Based:-

The algorithms like PCA and Fisher's Discriminant can be used to define the subspace representing facial patterns. There is a trained classifier, which correctly identifies instances of the target pattern class from the background image patterns.

4.3.Neural-Networks:-

Many detection problems like object detection, face detection, emotion detection, and face recognition, etc. have been faced successfully by Neural Networks.

4.4.Support Vector Machine:-

Support Vector Machines are linear classifiers that maximise the margin between the decision hyperplane and the examples in the training set. Osuna et al. first applied this classifier to face detection.

4.5.Sparse Network of Winnows:-

They defined a sparse network of two linear units or target nodes; one represents face patterns and other for the non-face patterns. It is less time consuming and efficient.

4.6.Naive Bayes Classifiers:-

They computed the probability of a face to be present in the picture by counting the frequency of occurrence of a series of the pattern over the training images. The classifier captured the joint statistics of local appearance and position of the faces.

4.7.Hidden Markov Model:-

The states of the model would be the facial features, which usually described as a set of pixels. HMM's commonly used along with other

methods to build detection algorithms.

4.8.Information Theoretical Approach:-

Markov Random Fields (MRF) can use for face pattern and correlated features. The Markov process maximises the discrimination between classes using Kullback-Leibler divergence. Therefore this method can be used in Face Detection.

4.9.Inductive Learning:-

This approach has been used to detect faces. Algorithms like Quinlan's C4.5 or Mitchell's FIND-S used for this purpose.

How the Face Detection Works:-

There are many techniques to detect faces, with the help of these techniques, we can identify faces with higher accuracy. These techniques have an almost same procedure for Face Detection such as OpenCV, Neural Networks, Matlab, etc. The face detection work as to detect multiple faces in an image. Here we work on OpenCV for Face Detection, and there are some steps that how face detection operates, which are as follows-

Firstly the image is imported by providing the location of the image. Then the picture is transformed from RGB to Grayscale because it is easy to detect faces in the grayscale.

Top highlight



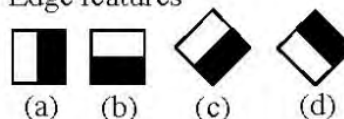
Converting RGB image to Grayscale

After that, the image manipulation used, in which the resizing, cropping, blurring and sharpening of the images done if needed. The next step is image segmentation, which is used for contour detection or segments the multiple objects in a single image so that the classifier can quickly detect the objects and faces in the picture.

The next step is to use Haar-Like features algorithm, which is proposed by Viola and Jones for face detection. This algorithm used for finding the location of the human faces in a frame or image. All human faces shares some universal properties of the human face like the eyes region is darker than its neighbour pixels and nose region is brighter than eye region.



Edge features



#1197



Line features



(a)



(b)



(c)



(d)



(e)



(f)



(g)



(h)

Center-surround features



(a)



(b)

Haar-like features for face detection

The haar-like algorithm is also used for feature selection or feature extraction for an object in an image, with the help of edge detection, line detection, centre detection for detecting eyes, nose, mouth, etc. in the picture. It is used to select the essential features in an image and extract these features for face detection.

The next step is to give the coordinates of x, y, w, h which makes a rectangle box in the picture to show the location of the face or we can say that to show the region of interest in the image. After this, it can make a rectangle box in the area of interest where it detects the face. There are also many other detection techniques that are used together for detection such as smile detection, eye detection, blink detection, etc.



Successfully detect the face in an image

How to Run Face Detector in Real-Time (Webcam):-

Requirement for Running the code- Python, OpenCV, Webcam, Numpy.

```
#import libraries
import cv2
import numpy as np

#import classifier for face and eye detection
face_classifier =
cv2.CascadeClassifier('Haarcascades/haarcascade_frontalface_default.x
ml')

# Import Classifier for Face and Eye Detection
face_classifier =
cv2.CascadeClassifier('Haarcascades/haarcascade_frontalface_default.x
```

```

ml)
eye_classifier = cv2.CascadeClassifier(
('Haarcascades/haarcascade_eye.xml'))
def face_detector (img, size=0.5):

    # Convert Image to Grayscale
    gray = cv2.cvtColor (img, cv2.COLOR_BGR2GRAY)
    faces = face_classifier.detectMultiScale (gray, 1.3, 5)
    If faces is ():
    return img

    # Given coordinates to detect face and eyes location from ROI
    for (x, y, w, h) in faces
    x = x - 100
    w = w + 100
    y = y - 100
    h = h + 100
    cv2.rectangle (img, (x, y), (x+w, y+h), (255, 0, 0), 2)
    roi_gray = gray[y: y+h, x: x+w]
    roi_color = img[y: y+h, x: x+w]
    eyes = eye_classifier.detectMultiScale (roi_gray)
    for (ex, ey, ew, eh) in eyes:
    cv2.rectangle(roi_color,(ex,ey),(ex+ew,ey+eh),(0,0,255),2)
    roi_color = cv2.flip (roi_color, 1)
    return roi_color

    # Webcam setup for Face Detection
    cap = cv2.VideoCapture (0)
    while True:
    ret, frame = cap.read ()
    cv2.imshow ('Our Face Extractor', face_detector (frame))
    if cv2.waitKey (1) == 13: #13 is the Enter Key
    break

    # When everything done, release the capture
    cap.release ()
    cv2.destroyAllWindows ()


```

This blog is for beginners who want to start their carrier in the field of Computer Vision or AI by learning about what is face detection, its types, and how it is work.

Sign up for The Variable

By Towards Data Science

Every Thursday, the Variable delivers the very best of Towards Data Science: from hands-on tutorials and cutting-edge research to original features you don't want to miss. [Take a look.](#)

 Get this newsletter

Facedetection Machine Learning Computer Vision Opencv Data Science

 1.3K  8



More from Towards Data Science

Follow

Your home for data science. A Medium publication sharing concepts, ideas and codes.

Joanne Jordan · Apr 27, 2018 ★

From Failed Passage to Rite of Passage: The Titanic Data Set as a Data Science Educational Tool

The sinking of the RMS Titanic is one of the most well known tragedies of

modern history. Its place as an event of note in history was in large part due to its 1997 retelling as a movie in which the Titanic acted both as the setting and the movie...

Read more · 4 min read



Share your ideas with millions of readers.

Write on Medium

TDS Editors · Apr 27, 2018

EXHIBIT 8



Search EnterpriseAI

TOPIC ▼
Machine learning
platformsSUBTOPIC ▼
Pattern recognition and
machine learning

Search the TechTarget Network

[Home](#) > [Pattern recognition and machine learning](#) > [Artificial intelligence - machine learning](#) > [face detection](#)

DEFINITION

face detection



By Corinne Bernstein

Face detection -- also called facial detection -- is an [artificial intelligence](#) (AI) based computer technology used to find and identify human faces in digital images. Face detection technology can be applied to various fields -- including security, [biometrics](#), law enforcement, entertainment and personal safety -- to provide surveillance and tracking of people in real time.

Face detection has progressed from rudimentary [computer vision](#) techniques to advances in machine learning (ML) to increasingly sophisticated artificial neural networks (ANN) and related technologies; the result has been continuous performance improvements. It now plays an important role as the first step in many key applications -- including face tracking, face analysis and [facial recognition](#). Face detection has a significant effect on how sequential operations will perform in the application.

In face analysis, face detection helps identify which parts of an image or video should be focused on to determine age, gender and emotions using facial expressions. In a facial recognition system -- which maps an individual's facial features mathematically and stores the data as a faceprint -- face detection data is required for the [algorithms](#) that discern which parts of an image or video are needed to generate a faceprint. Once identified, the new faceprint can be compared with stored faceprints to determine if there is a match.

How face detection works

Face detection applications use algorithms and ML to find human faces within larger images, which often incorporate other non-face objects such as landscapes, buildings and other human body parts like feet or hands. Face detection algorithms typically start by searching for human eyes -- one of the easiest features to detect. The algorithm might then attempt to detect eyebrows, the mouth, nose, nostrils and the iris. Once the algorithm concludes that it has found a facial region, it applies additional tests to confirm that it has, in fact, detected a face.

To help ensure accuracy, the algorithms need to be trained on large [data sets](#) incorporating hundreds of thousands of positive and negative images. The training improves the algorithms' ability to determine whether there are faces in an image and where they are.

The methods used in face detection can be knowledge-based, feature-based, template matching or appearance-based. Each has advantages and disadvantages:

- Knowledge-based, or rule-based methods, describe a face based on rules. The challenge of this approach is the difficulty of coming up with well-defined rules.
- Feature invariant methods -- which use features such as a person's eyes or nose to detect a face -- can be negatively affected by noise and light.
- Template-matching methods are based on comparing images with standard face patterns or features that have been stored previously and correlating the two to detect a face. Unfortunately these methods do not address variations in pose, scale and shape.

Sponsored News

[Three Tenets of Security Protection for State and Local Government and Education](#)
--Dell Technologies

[Software Protection Isn't Enough for the Malicious New Breed of Low-Level ...](#)
--Intel

[See More](#)

Vendor Resources

[Biometrics in the enterprise: An opportunity or an ethical minefield?](#)
--ComputerWeekly.com

[CIO Trends #11: Benelux](#)
--ComputerWeekly.com

- Appearance-based methods employ statistical analysis and machine learning to find the relevant characteristics of face images. This method, also used in feature extraction for face recognition, is divided into sub-methods.

Some of the more specific techniques used in face detection include:

- Removing the background. For example, if an image has a plain, mono-color background or a pre-defined, static background, then removing the background can help reveal the face boundaries.
- In color images, sometimes skin color can be used to find faces; however, this may not work with all complexions.
- Using motion to find faces is another option. In real-time video, a face is almost always moving, so users of this method must calculate the moving area. One drawback of this method is the risk of confusion with other objects moving in the background.
- A combination of the strategies listed above can provide a comprehensive face detection method.

Detecting faces in pictures can be complicated due to the variability of factors such as pose, expression, position and orientation, skin color and pixel values, the presence of glasses or facial hair, and differences in camera gain, lighting conditions and image resolution. Recent years have brought advances in face detection using [deep learning](#), which presents the advantage of significantly outperforming traditional computer vision methods.

Major improvements to face detection methodology came in 2001, when computer vision researchers Paul Viola and Michael Jones proposed a framework to detect faces in [real time](#) with high accuracy. The Viola-Jones framework is based on training a model to understand what is and is not a face. 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.

Although the Viola-Jones framework is still popular for recognizing faces in real-time applications, it has limitations. For example, the framework might not work if a face is covered with a mask or scarf, or if a face is not properly oriented, then the algorithm might not be able to find it.

To help eliminate the drawbacks of the Viola-Jones framework and improve face detection, other algorithms -- such as region-based convolutional neural network (R-CNN) and Single Shot Detector (SSD) -- have been developed to help improve processes.

A [convolutional neural network](#) (CNN) is a type of artificial neural network used in [image recognition](#) and processing that is specifically designed to process pixel data. An R-CNN generates region proposals on a CNN framework to localize and classify objects in images.

While region proposal network-based approaches such as R-CNN need two shots -- one for generating region proposals and one for detecting the object of each proposal -- SSD only requires one shot to detect multiple objects within the image. Therefore, SSD is significantly faster than R-CNN.

Advantages of face detection

As a key element in facial imaging applications, such as facial recognition and face analysis, face detection creates various advantages for users, including:

- Improved security. Face detection improves surveillance efforts and helps track down criminals and terrorists. Personal security is also enhanced since there is nothing for hackers to steal or change, such as passwords.

- Easy to integrate. Face detection and facial recognition technology is easy to integrate, and most solutions are compatible with the majority of security software.
- Automated identification. In the past, identification was manually performed by a person; this was inefficient and frequently inaccurate. Face detection allows the identification process to be automated, thus saving time and increasing accuracy.

Disadvantages of face detection

While face detection provides several large benefits to users, it also holds various disadvantages, including:

- Massive data storage burden. The ML technology used in face detection requires powerful [data storage](#) that may not be available to all users.
- Detection is vulnerable. While face detection provides more accurate results than manual identification processes, it can also be more easily thrown off by changes in appearance or camera angles.
- A potential breach of privacy. Face detection's ability to help the government track down criminals creates huge benefits; however, the same surveillance can allow the government to observe private citizens. Strict regulations must be set to ensure the technology is used fairly and in [compliance](#) with human privacy rights.

Face detection vs. face recognition

Although the terms *face detection* and *face recognition* are often used together, facial recognition is only one application for face detection -- albeit one of the most significant ones. Facial recognition is used for unlocking phones and mobile apps as well as for Biometric verification. The banking, retail and transportation-security industries employ facial recognition to reduce crime and prevent violence.

In short, the term *face recognition* extends beyond detecting the presence of a human face to determine whose face it is. The process uses a computer application that captures a digital image of an individual's face -- sometimes taken from a video frame -- and compares it to images in a database of stored records.

Uses of face detection

Although all facial recognition systems use face detection, not all face detection systems are used for facial recognition. Face detection can also be applied for facial motion capture, or the process of electronically converting a human's facial movements into a digital database using cameras or laser scanners. This database can be used to produce realistic computer animation for movies, games or avatars.

Face detection can also be used to auto-focus cameras or to count how many people have entered an area. The technology also has marketing applications -- for example, displaying specific advertisements when a particular face is recognized.

Another application for face detection is as part of a software implementation of emotional inference, which can, for example, be used to help people with autism understand the feelings of people around them. The program "reads" the emotions on a human face using advanced image processing.

An additional use is drawing language inferences from visual cues, or "lip reading." This can help computers determine who is speaking, which may be helpful in security applications. Furthermore, face detection can be used to help determine which parts of an image to blur to assure privacy.

Continue Reading About face detection

- London Police is deploying facial recognition technology for surveillance
- Use of facial recognition in healthcare improves hospital security
- Bypassing facial recognition: The means, motive and opportunity
- What are the most common digital authentication methods?
- Retail facial recognition and eye tracking the next tech wave, maybe

Related Terms

narrow AI (weak AI)

Narrow AI is an application of artificial intelligence technologies to enable a high-functioning system that replicates -- and ... [See complete definition](#)

recurrent neural networks

A recurrent neural network (RNN) is a type of artificial neural network commonly used in speech recognition and natural language ... [See complete definition](#)

What is artificial intelligence?

Artificial intelligence is the simulation of human intelligence processes by machines, especially computer systems. Specific ... [See complete definition](#)

Dig Deeper on Pattern recognition and machine learning

Yoti develops age estimation algorithm for under-13s



By: Sebastian Klovig S...

Time to take a step back on police use of facial recognition



By: Bryan Glick

What is a neural network? Explanation and examples



By: Ed Burns

CNN vs. RNN: How are they different?



By: David Petersson

resources

BUSINESS ANALYTICS



CIO

DATA MANAGEMENT

ERP



The roadblocks of business intelligence growth

Training and cost are the two biggest business intelligence challenges impeding organizations' BI usage and expansion, according ...



Looker adds customization capabilities to analytics platform

In concert with its virtual user conference, the vendor introduced the idea of composable analytics, along with tools that enable...



Tableau makes data literacy a priority with new pledge

As organizations increasingly turn to data to inform decisions, more data workers are needed. To address demand, Tableau pledged ...



About Us

Editorial Ethics Policy

Meet The Editors

Contact Us

Advertisers

Business Partners

Media Kit

Corporate Site

Contributors

Reprints

Answers

Definitions

E-Products

Events

Features

Guides

Opinions

Photo Stories

Quizzes

Tips

Tutorials

Videos

All Rights Reserved. Copyright
2018 - 2021, TechTarget.

Privacy Policy
Do Not Sell My Personal Info

EXHIBIT 9

Cascade Classifier

Next Tutorial: [Cascade Classifier Training](#)

Goal

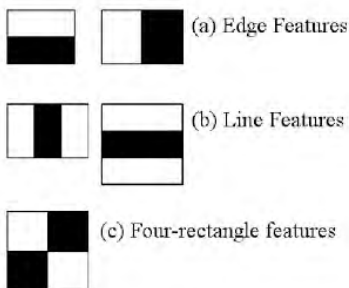
In this tutorial,

- We will learn how the Haar cascade object detection works.
- We will see the basics of face detection and eye detection using the Haar Feature-based Cascade Classifiers
- We will use the `cv::CascadeClassifier` class to detect objects in a video stream. Particularly, we will use the functions:
 - `cv::CascadeClassifier::load` to load a .xml classifier file. It can be either a Haar or a LBP classifier
 - `cv::CascadeClassifier::detectMultiScale` to perform the detection.

Theory

Object Detection using Haar feature-based cascade classifiers is an effective object detection method proposed by Paul Viola and Michael Jones in their paper, "Rapid Object Detection using a Boosted Cascade of Simple Features" in 2001. It is a machine learning based approach where a cascade function is trained from a lot of positive and negative images. It is then used to detect objects in other images.

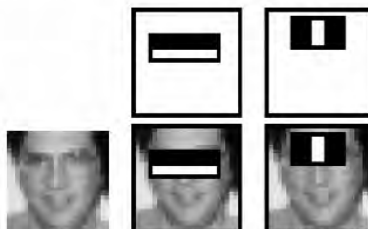
Here we will work with face detection. Initially, the algorithm needs a lot of positive images (images of faces) and negative images (images without faces) to train the classifier. Then we need to extract features from it. For this, Haar features shown in the below image are used. They are just like our convolutional kernel. Each feature is a single value obtained by subtracting sum of pixels under the white rectangle from sum of pixels under the black rectangle.



image

Now, all possible sizes and locations of each kernel are used to calculate lots of features. (Just imagine how much computation it needs? Even a 24x24 window results over 160000 features). For each feature calculation, we need to find the sum of the pixels under white and black rectangles. To solve this, they introduced the integral image. However large your image, it reduces the calculations for a given pixel to an operation involving just four pixels. Nice, isn't it? It makes things super-fast.

But among all these features we calculated, most of them are irrelevant. For example, consider the image below. The top row shows two good features. The first feature selected seems to focus on the property that the region of the eyes is often darker than the region of the nose and cheeks. The second feature selected relies on the property that the eyes are darker than the bridge of the nose. But the same windows applied to cheeks or any other place is irrelevant. So how do we select the best features out of 160000+ features? It is achieved by **Adaboost**.



image

For this, we apply each and every feature on all the training images. For each feature, it finds the best threshold which will classify the faces to positive and negative. Obviously, there will be errors or misclassifications. We select the features with minimum error rate, which means they are the features that most accurately classify the face and non-face images. (The process is not as simple as this. Each image is given an equal weight in the beginning. After each classification, weights of misclassified images are increased. Then the same process is done. New error rates are calculated. Also new weights. The process is continued until the required accuracy or error rate is achieved or the required number of features are found).

The final classifier is a weighted sum of these weak classifiers. It is called weak because it alone can't classify the image, but together with others forms a strong classifier. The paper says even 200 features provide detection with 95% accuracy. Their final setup had around 6000 features. (Imagine a reduction from 160000+ features to 6000 features. That is a big gain).

So now you take an image. Take each 24x24 window. Apply 6000 features to it. Check if it is face or not. Wow.. Isn't it a little inefficient and time consuming?

Yes, it is. The authors have a good solution for that.

In an image, most of the image is non-face region. So it is a better idea to have a simple method to check if a window is not a face region. If it is not, discard it in a single shot, and don't process it again. Instead, focus on regions where there can be a face. This way, we spend more time checking possible face regions.

For this they introduced the concept of **Cascade of Classifiers**. Instead of applying all 6000 features on a window, the features are grouped into different stages of classifiers and applied one-by-one. (Normally the first few stages will contain very many fewer features). If a window fails the first stage, discard it. We don't consider the remaining features on it. If it passes, apply the second stage of features and continue the process. The window which passes all stages is a face region. How is that plan?

The authors' detector had 6000+ features with 38 stages with 1, 10, 25, 25 and 50 features in the first five stages. (The two features in the above image are actually obtained as the best two features from Adaboost). According to the authors, on average 10 features out of 6000+ are evaluated per sub-window.

So this is a simple intuitive explanation of how Viola-Jones face detection works. Read the paper for more details or check out the references in the Additional Resources section.

Haar-cascade Detection in OpenCV

C++ Java Python

OpenCV provides a training method (see [Cascade Classifier Training](#)) or pretrained models, that can be read using the `cv::CascadeClassifier::load` method. The pretrained models are located in the data folder in the OpenCV installation or can be found [here](#).

The following code example will use pretrained Haar cascade models to detect faces and eyes in an image. First, a `cv::CascadeClassifier` is created and the necessary XML file is loaded using the `cv::CascadeClassifier::load` method. Afterwards, the detection is done using the `cv::CascadeClassifier::detectMultiScale` method, which returns boundary rectangles for the detected faces or eyes.

This tutorial code's is shown lines below. You can also download it from [here](#)

```
#include "opencv2/objdetect.hpp"
#include "opencv2/highgui.hpp"
#include "opencv2/imgproc.hpp"
#include "opencv2/videoio.hpp"
#include <iostream>

using namespace std;
using namespace cv;

void detectAndDisplay( Mat frame );

CascadeClassifier face_cascade;
CascadeClassifier eyes_cascade;

int main( int argc, const char** argv )
{
    CommandLineParser parser(argc, argv,
        "{help h|}"
        "{face_cascade|data/haarcascades/haarcascade_frontalface_alt.xml|Path to face cascade.}"
        "{eyes_cascade|data/haarcascades/haarcascade_eye_tree_eyeglasses.xml|Path to eyes cascade.}"
        "{camera|0|Camera device number.}");

    parser.about( "\nThis program demonstrates using the cv::CascadeClassifier class to detect objects (Face + eyes) in a video\nstream.\n\n"
        "You can use Haar or LBP features.\n\n" );
    parser.printMessage();

    String face_cascade_name = samples::findFile( parser.get<String>("face_cascade") );
    String eyes_cascade_name = samples::findFile( parser.get<String>("eyes_cascade") );

    //-- 1. Load the cascades
    if( !face_cascade.load( face_cascade_name ) )
    {
        cout << "--(!)Error loading face cascade\n";
        return -1;
    };
    if( !eyes_cascade.load( eyes_cascade_name ) )
    {
        cout << "--(!)Error loading eyes cascade\n";
        return -1;
    };

    int camera_device = parser.get<int>("camera");
    VideoCapture capture;
    //-- 2. Read the video stream
    capture.open( camera_device );
    if ( ! capture.isOpened() )
    {
        cout << "--(!)Error opening video capture\n";
        return -1;
    }

    Mat frame;
    while ( capture.read(frame) )
    {
        if( frame.empty() )
        {
            cout << "--(!) No captured frame -- Break!\n";
            break;
        }

        //-- 3. Apply the classifier to the frame
        detectAndDisplay( frame );

        if( waitKey(10) == 27 )
        {
            break; // escape
        }
    }
}
```

```

}

void detectAndDisplay( Mat frame )
{
    Mat frame_gray;
    cvtColor( frame, frame_gray, COLOR_BGR2GRAY );
    equalizeHist( frame_gray, frame_gray );

    //-- Detect faces
    std::vector<Rect> faces;
    face_cascade.detectMultiScale( frame_gray, faces );

    for ( size_t i = 0; i < faces.size(); i++ )
    {
        Point center( faces[i].x + faces[i].width/2, faces[i].y + faces[i].height/2 );
        ellipse( frame, center, Size( faces[i].width/2, faces[i].height/2 ), 0, 0, 360, Scalar( 255, 0, 255 ), 4 );

        Mat faceROI = frame_gray( faces[i] );

        //-- In each face, detect eyes
        std::vector<Rect> eyes;
        eyes_cascade.detectMultiScale( faceROI, eyes );

        for ( size_t j = 0; j < eyes.size(); j++ )
        {
            Point eye_center( faces[i].x + eyes[j].x + eyes[j].width/2, faces[i].y + eyes[j].y + eyes[j].height/2 );
            int radius = cvRound( (eyes[j].width + eyes[j].height)*0.25 );
            circle( frame, eye_center, radius, Scalar( 255, 0, 0 ), 4 );
        }
    }

    //-- Show what you got
    imshow( "Capture - Face detection", frame );
}

```

Result

1. Here is the result of running the code above and using as input the video stream of a built-in webcam:



Be sure the program will find the path of files *haarcascade_frontalface_alt.xml* and *haarcascade_eye_tree_eyeglasses.xml*. They are located in *opencv/data/haarcascades*

2. This is the result of using the file *lbpcascade_frontalface.xml* (LBP trained) for the face detection. For the eyes we keep using the file used in the tutorial.



Additional Resources

1. Paul Viola and Michael J. Jones. Robust real-time face detection. International Journal of Computer Vision, 57(2):137–154, 2004. [224]
2. Rainer Lienhart and Jochen Maydt. An extended set of haar-like features for rapid object detection. In Image Processing. 2002. Proceedings. 2002 International Conference on, volume 1, pages I–900. IEEE, 2002. [132]
3. Video Lecture on Face Detection and Tracking
4. An interesting interview regarding Face Detection by Adam Harvey
5. OpenCV Face Detection: Visualized on Vimeo by Adam Harvey

EXHIBIT 10

Overview

Things

Story

Abstract

Instructions

Code

Credits

Comments (3)

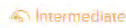
 81

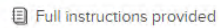

Keval Doshi

Published April 26, 2017 © GPL3+

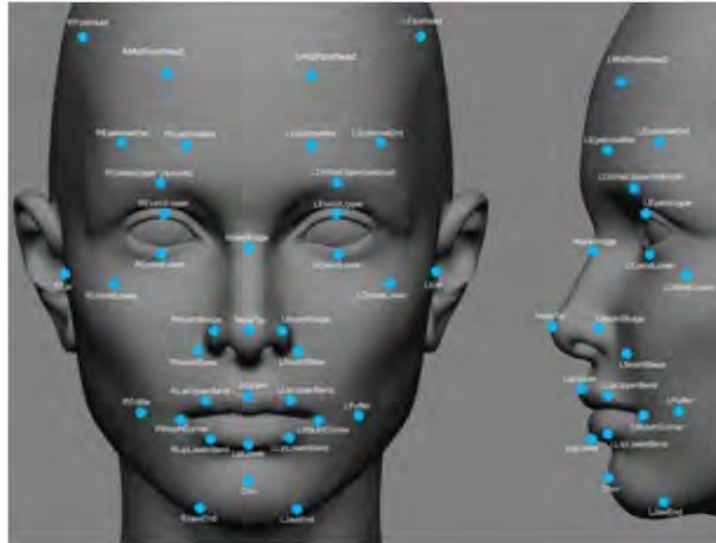
Face Detection using Raspberry Pi and Smartphone

Face Detection is really awesome! This is a tutorial about making a very cheap face detection system.

 Intermediate

 Full instructions provided

 2 hours

 12,674


SAMSUNG



Take the AXDMM challenge!

Your imagination could win \$60,000.

LEARN MORE



RELATED CHANNELS AND TAGS



facial recognition

image processing

RELATED PROJECTS



Face Detection with OpenVINO on Raspberry Pi



Face Recognition Using Mathworks on Raspberry Pi



Face to Voice | Visually Impaired | Raspberry Pi

Things used in this project

Hardware components



Raspberry Pi 3 Model B

× 1



Raspberry Pi Camera Module

× 1



Story

Abstract:

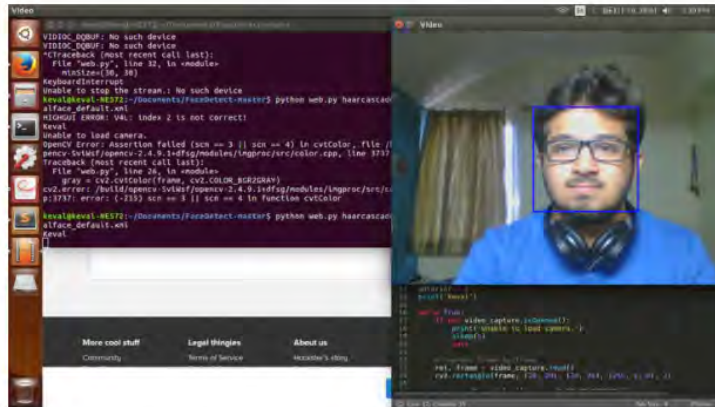
Face detection seems to be a very complex idea, but in reality it is really simple.

Prerequisites:

- Raspberry Pi 2 or 3 with Raspbian OS installed
- Raspberry Pi Camera module or your Smartphone
- Basic Python knowledge

Instructions:

1. The first thing to do is install OpenCV. How to install OpenCV is instructed [here](#). #1213
2. Attach the Raspberry Pi Camera Module. Go to Raspi-config from the terminal and switch camera interface on.
3. The Python code for Face detection is given attached.
4. Open a terminal and run the Python script.

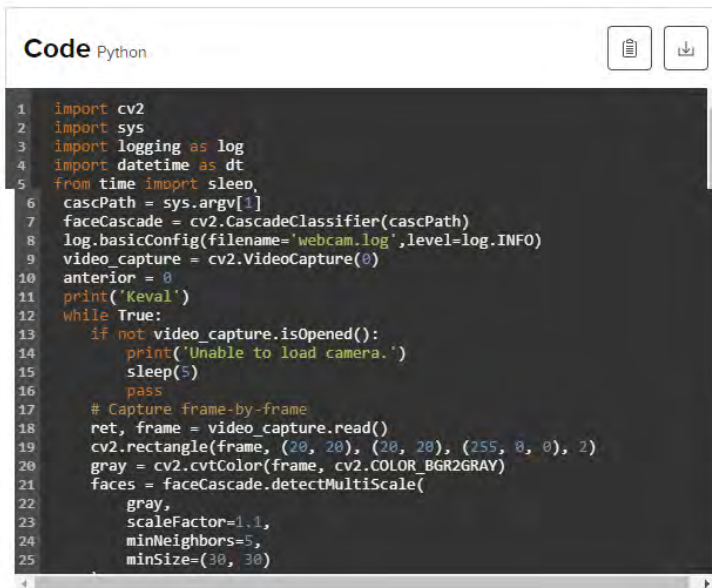


5. For those using a Smartphone for camera, download IP Webcam from Playstore. After that make the following change in the Python file:

```
video_capture = cv2.VideoCapture("http://192.168.43.1:8080/video")
```

And voila!

Code



Credits



Keval Doshi

1 project • 26 followers

Hardware Hacker. Love going to hackathons. Enough said!

Follow

Contact

Comments

Please [log in](#) or [sign up](#) to comment.

Darshan V.M

3 years ago

hey i got an error bro while running python script
Traceback (most recent call last):
File "/home/pi/recongnize.py", line 6, in <module>
cascPath = sys.argv[1]
IndexError: list index out of range

[1](#) thank

EXHIBIT 11



Privacy Policy

Privacy Policy

This Privacy Policy is effective as of July 21, 2021.

This Privacy Policy relates to Lytx, Inc., together with its affiliates (collectively, "Lytx", "we", "us" and/or "our"), and describes our policies and practices with respect to your personal information ("Personal Information") that you may give us or that we may collect about you, such as (i) when using our website or Lytx Mobile Application ("Mobile App") which contain a link to this policy, (ii) when entering information into an online form which contains a link to this Privacy Policy, (iii) when providing your Personal Information to a Lytx representative at a tradeshow, or (iv) when you otherwise provide Lytx with your Personal Information in a manner described in this Privacy Policy.

This Privacy Policy does not apply to the extent we process Personal Information in our role as a service provider on behalf of our clients. For detailed privacy information related to a Lytx client's use of Lytx website and Mobile App, please direct your inquiry to the respective client. We are not responsible for the privacy or data security practices of our clients, which may differ from those set forth in this Privacy Policy.

This Privacy Policy also does not apply to the Personal Information obtained from or related to our current and former employees, independent contractors, and applicants. Please see Lytx's [Human Capital Privacy Policy](#) for more information related to Personal Information obtained from or related to our current and former employees, independent contractors, and applicants. This [Human Capital Privacy Policy](#) also applies to any beneficiaries or emergency contacts of Lytx employees, independent contractors, or applicants who are California residents.

By submitting information via any method on our website or through our Mobile App, which includes a link or reference to this policy you acknowledge that Lytx will collect, use, share, transfer, and store Personal Information in the manner described in this Privacy Policy.

A Special Note for Parents Concerning Privacy

The Lytx website and Mobile App are not intended for use by children. We do not knowingly accept Personal Information from any person under the age of 13. We ask that children (under the age of 13) do not submit any Personal Information to us.

Information We Collect

The Personal Information we collect depends on how you interact with us, the website and Mobile App you use, and the choices you make.

We may collect information about you from different sources and in various ways when you use our services, including information you provide directly, information collected automatically, third-party data sources, and data we infer or generate from other data.

Information you provide directly. We collect Personal Information you provide to us. For example:

- **Contact Information:** for example, if you express an interest in obtaining additional information about our services, request customer support, use our "Contact Us" or similar features, register to use our website and Mobile App, sign up for or attend an event or webinar, or download certain content, we generally require you to provide us with your contact information, such as your name, job title, company name, address, phone number, or email address;
- **Demographic Information:** for example, in some cases, such as when you register or participate in surveys, we may collect age, gender, marital status, and similar demographic details;
- **Financial Information:** for example, if you make purchases via our website and Mobile App or register for an event, we may also require you to provide us (or our service providers who provide payment processing services) with financial information and billing information, such as billing name and address, credit card number, or bank account information;
- **Content and Files:** for example if you contact us via telephone or email, we will collect and retain those communications (or records relating to those communications or if you participate in a survey we may collect information you submit related to your use of our website and Mobile App; or

Information we collect automatically. When you use our website and Mobile App, we collect some information automatically. For example:

- **Identifiers and device information.** When you access or use our website and Mobile App, our web servers automatically log your Internet Protocol (IP) address and information about your device, including device identifiers (such as MAC address); device type; and your device's operating system, browser, and other software including type, version, language, settings, and configuration. As further described in the Cookies, Mobile IDs, and Similar Technologies section below, our websites and online services store and retrieve cookie identifiers, mobile IDs, and other data.
- **Geolocation data.** Depending on your device and app settings, we collect precise geolocation data when you use our apps or online services.

- **Usage data.** We automatically log your activity on our websites, apps and connected products, including the URL of the website from which you came to our sites, pages you viewed, how long you spent on a page, access times, and other details about your use of and actions on our website.

Information we create or generate. We may infer new information from other data we collect, including using automated means to generate information about your likely preferences or other characteristics (“**inferences**”). For example, we may infer your general geographic location (such as city, state, and country) based on your IP address.

Cookies, Mobile IDs and Similar Technologies

What are cookies and similar technologies?

Cookies are small text files placed by a website and stored by your browser on your device. A cookie can later be read when your browser connects to a web server in the same domain that placed the cookie. The text in a cookie contains a string of numbers and letters that may uniquely identify your device and can contain other information as well. This allows the web server to recognize your browser over time, each time it connects to that web server.

Web beacons are electronic images (also called single-pixel or clear GIFs) that are contained within a website or email. When your browser opens a webpage or email that contains a web beacon, it automatically connects to the web server that hosts the image (typically operated by a third party). This allows that web server to log information about your device and to set and read its own cookies. In the same way, third-party content on our websites (such as embedded videos, plug-ins, or ads) results in your browser connecting to the third-party web server that hosts that content. We also include web beacons in our email messages or newsletters to tell us if you open and act on them.

Mobile analytics and advertising IDs are generated by operating systems for mobile devices (iOS and Android) and can be accessed and used by apps in much the same way that websites access and use cookies. Our apps contain software that enables us and our third-party analytics and advertising partners to access the mobile IDs.

How do we and our partners use cookies and similar technologies?

We, and our analytics and advertising partners, use these technologies in our websites, apps, and online services to collect Personal Information (such as the pages you visit, the links you click on, and similar usage information, identifiers, and device information) when you use our services, including Personal Information about your online activities over time and across different websites or online services. This information is used to store your preferences and settings, enable you to sign-in, analyze how our websites and apps perform, track your interaction with the site or app, develop inferences, deliver and tailor interest-based advertising, combat fraud, and fulfill other legitimate purposes. We and/or our partners also share the information we collect or infer with third parties for these purposes.

What controls are available?

- **Advertising controls.** Our advertising partners may participate in association that provide simple ways to opt out of ad targeting, which you can access at:
 - United States: NAI (<http://optout.networkadvertising.org>) and DAA (<http://optout.aboutads.info/>)
 - Canada: Digital Advertising Alliance of Canada (<https://youradchoices.ca/>)
 - Europe: European Digital Advertising Alliance (<http://www.youonlinechoices.com/>)

These choices are specific to the browser you are using. If you access our services from other devices or browsers, take these actions from those systems to ensure your choices apply to the data collected when you use those systems.

- **Browser cookie controls.** Most web browsers are set to accept cookies by default. If you prefer, you can go to your browser settings to learn how to delete or reject cookies. If you choose to delete or reject cookies, this could affect certain features or services of our website. If you choose to delete cookies, settings and preferences controlled by those cookies, including advertising preferences, may be deleted and may need to be recreated.
- **Mobile advertising ID controls.** iOS and Android operating systems provide options to limit tracking and/or reset the advertising IDs.
- **Email web beacons.** Most email clients have settings which allow you to prevent the automatic downloading of images, including web beacons, which prevents the automatic connection to the web servers that host those images.
- **Do Not Track.** Some browsers have incorporated “Do Not Track” (DNT) features that can send a signal to the websites you visit indicating you do not wish to be tracked. Because there is not a common understanding of how to interpret the DNT signal, our websites do not currently respond to browser DNT signals. Instead, you can use the range of other tools to control data collection and use, including the cookie controls and advertising controls described above.

California “Do Not Sell My Personal Information”

The California Consumer Protection Act (“CCPA”) requires us to describe the categories of Personal Information we sell to third parties and how to opt-out of future sales. The CCPA defines Personal Information to include online identifiers, including IP addresses, cookies IDs, and mobile IDs. The law also defines a “sale” broadly to include simply making data available to third parties in some cases. We let advertising and analytics providers collect IP addresses, cookie IDs, and mobile IDs, along with associated device and usage data, when you access our online services, but we do not “sell” any other Personal Information.

If you do not wish for us or our partners to “sell” Personal Information relating to your visits to our sites for advertising purposes, you can make your Do Not Sell Request by emailing us or using the choices above in the previous section “What controls are available?” If you opt-out using these choices, we will not share or make available such Personal Information in ways that are considered a “sale” under the CCPA. However, we will continue to make available to our partners (acting as our service providers) some Personal Information to help us perform advertising-related functions. Further, using these choices will not opt you out of the use of previously “sold” Personal Information or stop all interest-based advertising.

Our Use of Personal Information

We use the Personal Information we collect for purposes described in this Privacy Policy or otherwise disclosed to you. For example, we use Personal Information for the following purposes:

- *Operating our website and Mobile App:* We base the processing of your Personal Information on our legitimate interest to operate and administer our website and Mobile App and to provide you with content you access and request (e.g., download of certain content from our website and Mobile App);
- *Analyzing and monitoring our website and Mobile App:* We will process Personal Information to analyze overall trends, to help us provide and improve our website and Mobile App and assess whether they are functioning properly;
- *Promoting security of our website and Mobile App:* We will process your Personal Information by monitoring use of our website and Mobile App, creating

aggregated, non-personal information, verifying accounts and activity, investigating suspicious activity, as well as violations of and enforcement of our terms and policies, to the extent this is necessary for the purpose of our legitimate interests in promoting the safety and security of the systems and application used for our website and Mobile App, and protecting our rights and the rights of others;

- *Handling contact and user support requests:* If you fill out a "Contact Us" web form, request user support, or if you contact us by other means, we will process your Personal Information for the performance of our contract with you and to the extent it is necessary for the purpose of our legitimate interests to fulfill your request and communicate with you;
- *Managing event registrations and attendance:* We will process your Personal Information to plan and host the event, conference or webinar, including related communication with you;
- *Business Operations:* We will process your Personal Information to operate our business, such as billing, accounting, improving our internal operations, securing our systems, detecting fraudulent or illegal activity, and meeting our legal obligations. For example, if you have provided financial information, Lytx, or its service provider, will process your respective Personal Information to check the financial qualifications and collect payments to the extent this is necessary for completing transaction with you under the purchase order submitted by you;
- *Providing Mobile App Services:* If you have installed and use our Mobile App, you provide us with GPS location information which is required in order for us to provide you with our Route Risk program. We also use other electronic information received from your mobile device to send updates to the Mobile App that includes driver safety tips.
- *Developing and improving our website and Mobile App:* We will process your Personal Information to analyze trends, track your usage of our website and Mobile App and interactions with emails to the extent this is necessary for our legitimate interests to develop and improve our website and Mobile App and to provide our users with more relevant and interesting content;
- *Displaying personalized advertisements and content:* We will process your Personal Information to conduct marketing research, advertise to you, provide personalized information about us on and off our website and Mobile App, and provide other personalized content based upon your activities and interests to the extent it is necessary for our legitimate interests to advertise our website and Mobile App or, where necessary, to the extent you have provided your prior separate consent;
- *Sending business communications:* We will process your Personal Information to send you information, including confirmations, invoices, technical notices, updates, security alerts, and support and administrative messages
- *Sending marketing communications:* We will process your Personal Information to send you marketing information, product recommendations and other non-transactional communications (e.g., marketing newsletters, SMS, or push notifications) about us and our affiliates and partners, including information about our products, promotions or events as necessary to conduct direct marketing or to the extent you have provided your prior separate consent; and
- *Complying with legal obligations:* We will process your Personal Information when cooperating with public and government authorities, courts or regulators in accordance with our legal obligations under applicable laws to the extent this requires the processing or disclosure of Personal Information to protect our rights, and is necessary for our legitimate interests to protect against misuse or abuse of our website and Mobile App, to protect personal property or safety, to pursue remedies available to us and limit our damages, to comply with a judicial proceedings, court order or legal process, and/or to respond to lawful requests.

Our Sharing of Personal Information

We share Personal Information with your consent or as necessary to complete your transactions or provide the website and Mobile App you have requested or authorized. For example, when you provide payment data to make a purchase, we will share that data with banks and other entities as necessary for payment processing, fraud prevention, credit risk reduction, or other related financial services.

In addition, we share each of the categories of Personal Information described above for the following business purposes:

- Our contracted service providers who provide services such as IT and system administration and hosting, credit card processing, research and analytics, marketing, customer support and data enrichment;
- If you use our website and Mobile App to register for an event or webinar, we may share your Personal Information with the entity responsible for organizing and/or managing the event to the extent this is required on the basis of the contract with you to process your registration and ensure your participation in the event;
- With third-party social networks, advertising networks and website and Mobile App, which usually act as separate controllers, so that we can market and advertise on third party platforms and website and Mobile App;
- In individual cases we may also share Personal Information with professional advisers acting as processors or joint controllers including lawyers, bankers, auditors and insurers based in countries in which we operate who provide consultancy, banking, legal, insurance and accounting services;
- We may also share your Personal Information with other affiliates to the extent this is necessary to fulfill a request you have submitted via our website and Mobile App, or for customer support, marketing, technical operations, or account management purposes;
- If we are involved in a merger or reorganization, sell a website or Mobile App, or business unit, or if all or a portion of our business, assets or stock are acquired by another company, we may transfer some or all of your Personal Information to such third party; or
- Any Personal Information or other information you choose to submit to public online forums (e.g. forums, blogs, or chat rooms) on our website and Mobile App may be read, collected, and/or used by others who visit these forums.

Lytx does not sell or trade any Personal Information accumulated through its website and Mobile App in any manner inconsistent with this Privacy Policy. However, Lytx, its partners, agents, officers and employees may provide specific information collected about you, including Personal Information, to third-parties if required to do so by law or in the good faith belief that such action is required to: (i) protect Lytx against legal liability; (ii) protect and defend the rights or property of Lytx, including without limitation, exchanging information with other companies and organizations for fraud protection or investigation; (iii) comply with a legal obligation; or (iv) act in urgent circumstances to protect the personal safety of visitors or the public.

Data collected from or about you may be used in an aggregate form, that is, as a statistical measure, and not in a form that would reasonably allow anyone to identify you. Along with using this data in aggregate form ourselves, we may share these statistics with certain strategic relations.

Your Privacy Rights

You may have certain rights regarding your Personal Information, subject to applicable privacy and data protection laws.

If you are a resident of the European Union, these may include the following rights:

- to access your Personal Information processed by us and receive copies of that information (right to access);
- to rectify inaccurate Personal Information and ensure it is complete (right to rectification);
- to erase/delete your Personal Information to the extent permitted by other legal obligations (right to erasure; right to be forgotten);
- to restrict our processing of your Personal Information (right to restriction of processing);
- to transfer your Personal Information to another controller to the extent possible (right to data portability);
- to object to any processing of your Personal Information carried out on the basis of our legitimate interests (right to object). Where we process your Personal Information for direct marketing purposes or share it with third parties for their own direct marketing purposes, you can exercise your right to object at any time to such processing without having to provide any specific reason for such objection;
- not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects ("Automated Decision-Making"); Automated Decision-Making is not currently implemented as part of our website and Mobile App; and
- to the extent we base the collection, processing and sharing of your Personal Information on your consent, to withdraw your consent at any time, without affecting the lawfulness of the processing based on such consent before its withdrawal.

If you are a resident of the state of California:

- You have a right to request that we disclose to you the Personal Information we have collected about you. You also have a right to request additional information about our collection, use, disclosure, or sale of such Personal Information. Note that we have provided much of this information in this Privacy Policy;
- You also have a right to request that we delete Personal Information under certain circumstances, subject to a number of exceptions. Please note, if your request relates to data processed by Lytx in connection with Lytx's role as a service provider for clients, you must direct your request to the client;
- You have the right to opt-out of the sale of your Personal Information, which is described in more detail in the above California "Do Not Sell My Personal Information" section;
- You have the right to not receive discriminatory treatment because you exercised any of your privacy rights; and
- You have the right to designate an authorized agent to make requests under the California Consumer Privacy Act; provided however that you must submit written proof of such designation to us and we may require additional verification.

We do not knowingly sell Personal Information of minors under 16 years of age.

To exercise your rights, please contact us either by email or mail in accordance with the "Contact" section below. Please note that we must verify any requests pursuant to this section to ensure the individual making such request is authorized to exercise such rights. Therefore, you must submit your name and email address, as well as confirm access to such email address, in order for us to process your request. Lytx will comply with the applicable privacy and data protection laws and the exercising of your rights under such laws, however please note that such rights specified above are not absolute, and exemptions may be applicable. We try to respond to all legitimate requests within one month and will contact you if we need additional information from you in order to honor your request. Occasionally it may take us longer than a month, taking into account the complexity and number of requests we receive.

Lytx may also process Personal Information in the role of a processor on behalf of Lytx clients' use of Lytx services. If your Personal Information has been submitted to us in connection with Lytx's provision of services to a client, and you wish to exercise any rights you may have under applicable data protection laws, please inquire with the specific client directly. Because we may only respond to a request related to our client's data with such client's permission, if you wish to make your request directly to us, please provide the name of the Lytx client who submitted your information when contacting us. We will refer your request to that client, and will support them as needed in responding to your request within a reasonable timeframe. If you are an employee of a Lytx client, we recommend you contact your company's system administrator for assistance in correcting or updating your information.

Preferences for Marketing Communications

If we process your Personal Information for the purpose of sending you marketing communications, you may manage your receipt of marketing and non-transactional communications from us by clicking on the "unsubscribe" link located on the bottom of our marketing emails, by replying or texting 'STOP' if you receive SMS communications, or by turning off push notifications on our apps on your device. Additionally, you may unsubscribe [here](#) or by contacting us using the information in the "Contact" section below. Please note that opting-out of marketing communications does not opt you out of receiving important business communications related to your current relationship with us, such as information about your subscriptions or event registrations, service announcements or security information.

Security

We take reasonable and appropriate steps to help protect Personal Information from unauthorized access, use, disclosure, alteration, and destruction.

International Transfer of Information Collected

Our servers, and service providers, are located in the United States. Accordingly, if you reside outside of the United States, by accessing or using our Products and Service, you agree that your information will be transferred to the United States, and processed and stored in the United States. You also acknowledge and agree that your information may be transferred to facilities of those third parties with whom we share data as described herein.

Individuals Located in the European Union: Your Personal Information may be processed outside the European Economic Area ("EEA"), and in countries which are not subject to an adequacy decision by the European Commission and which may not provide for the same level of data protection in the EEA. In this event, we will ensure that such recipient offers an adequate level of protection, for instance by entering into standard contractual clauses for the transfer of data as approved by the European Commission (Art. 46 GDPR), or we will ask you for your prior consent to such international data transfers. By submitting any of your Personal Information to the Products and Service(s), you consent and agree to the transfer of your Personal Information to Lytx and its affiliates, as well as Lytx's service

Limitation of Liability

By providing us with any Personal Information you expressly and unconditionally release and hold harmless Lytx, Inc., and its subsidiaries, affiliates, directors, officers, employees and agents from any and all liability for any injuries, loss or damage of any kind arising from or in connection with the use and/or misuse of your collected Personal Information. In addition, while Lytx takes efforts to ensure the proper and appropriate use of data provided by Lytx to third party companies, promotional partners or vendors, Lytx is not liable for any injuries, loss or damage of any kind arising from or in connection with the use and/or misuse of your collected Personal Information by Lytx or the above-mentioned non-Lytx entities. The foregoing shall not apply where such limitation of liability is prohibited by law.

Reservation of Rights

Lytx reserves the right to change this Privacy Policy at any time, for any reason, without prior notice. Your continued use of this website and Mobile App after any changes have taken effect will indicate that you have agreed to the terms of the revised Privacy Policy. We recommend that you check this Privacy Policy regularly for changes and updates.

External Links

Our website and Mobile App may include integrations, references, or links to services provided by third parties whose privacy practices differ from ours. If you provide Personal Information to any of those third parties, or allow us to share personal information with them, that information is governed by their privacy statements.

Other Legal Information and Terms and Conditions

Your access and use of this website and Mobile App is further subject to the terms and conditions at <https://www.lytx.com/legal-information>.

Changes in Corporate Structure

Notwithstanding any of the foregoing, Lytx may sell, share or otherwise transfer some or all of its assets, including information gathered by one of its websites, in connection with a bankruptcy, merger, acquisition, reorganization or sale of substantially all of its assets or substantially all of the assets of a division or other unit of Lytx. You acknowledge that such transfers may occur and that any acquirer may continue to use your Personal Information as set forth in this Privacy Policy.

Changes to this Privacy Statement

We will update this Privacy Policy when necessary to reflect changes in our website and Mobile App, how we process Personal Information, or the applicable law. When we post changes to the Privacy Policy, we will revise the "Last Updated" date at the top of the statement. If we make material changes to the Privacy Policy, we will provide notice or obtain consent regarding such changes as may be required by law.

How to Contact Us

If you have a privacy question, concern, or complaint, please contact the Lytx Privacy Department directly by e-mail at privacy@lytx.com. If you prefer to contact us by mail, please send any communications to:

Lytx, Inc.
9785 Towne Centre Drive
San Diego, California 92121
Attn: Chief Privacy Officer

Subscribe to our newsletter

Our Best Fleet Forward newsletter delivers monthly insights on fleet management.

First name

Get started today.

[1-866-419-5861](tel:1-866-419-5861) [Contact Us](#) [Book a Demo](#)

SOLUTIONS

[Fleet Management Overview](#)
[Fleet Dash Cams](#)
[Fleet Safety](#)

FEATURES

[DriveCam Event Recorder](#)
[Lytx Driver App](#)
[Machine Vision and Artificial](#)

SUPPORT & LOGIN

[Support](#)
[Lytx Account Login](#)
[Lytx Compliance Services \(RAIR\) Portal](#)

Last name

Email address

SUBMIT

tx

¹WARNING— The Lytx Drive Recorder is a driver aid only. Please wait for the device to provide a warning before taking measures to avoid an accident.
²Flowed time after. This service is provided at no cost for up to 7 requests. Fees for shipments of hardware may apply.
³Subject to available cellular network coverage.
⁴Estimate based upon tested sampling of Lytx/client data.
© Copyright Lytx, Inc. 2023. All rights reserved.

Fleet Tracking
DOT Compliance
ELD Compliance
FedEx VEDR
Lytx Integration Network

Fraudance
Risk ID Without Recording
Continual Behavior Reporting
Preventative Maintenance
Diagnostic Trouble Codes

Lytx DriveCam Academy
Parts Store

GUIDES

ADAS
CSA Scores
Defensive Driving for Commercial Fleets
Distracted Driving
DOT Regulations
ELD Guide
Fleet Maintenance
Fleet Management App
Fleet Management Solutions
Fleet Risk Management
Fuel Management Systems
Solutions to Texting and Driving
Telematics Systems

SITES

English (U.S.A.)
English (U.K.)

ABOUT US

Our Story
Our Technology
Our Team
Careers
News and Events
Who We Serve
Success Stories

RESOURCES

Blog
Buyer's Guide to Video Telematics
The Fleet Podcast
Videos
All Resources

[Site Map](#) [Legal](#) [Terms](#) [Privacy](#) [Driver Info](#)



EXHIBIT 12



PRESS RELEASE

Lytix Presents “State of the Data” Based on 100 Billion Miles of Driving Data

Trucking's commitment to safety shows in the data: 358,359 fewer risky events in 2018

SAN DIEGO and AUSTIN, Tex. – (Oct. 28, 2018) –

Lytix®, the world's leading provider of video telematics, analytics and safety solutions for commercial and public sector fleets, shared its State of the Data presentation today at the American Trucking Associations Management Conference and Exhibition (ATA MC&E), the premiere meeting for trucking executives. Based on 100 billion miles of driving data, the presentation focuses on truck-driving safety, risk factors and behaviors.

“With one hundred billion miles of driving data and our proprietary human-review processes, our ability to provide fleets with game-changing insights into their road- and site-based operations is unequalled,” said Brandon Nixon, Chairman and CEO of Lytx. “Our State of the Data presentation highlights behavioral trends and areas of opportunity to help keep truck drivers, cargo and our roadways even safer.”



Lytix Presents “State of the Data” Based on 100 Billion Miles of Driving Data

About the Data

Insights are derived from Lytx's trucking-industry client database. The data is anonymized, normalized and generalizable to the trucking industry as a whole, given Lytx's majority market share in video telematics solutions for commercial trucking industry at large.

Trucking is Getting Safer

Lytix trucking-industry data shows 358,359 fewer instances of risky driving between June-August 2018 compared to the same period in 2017. The following list reflects the top ten observed driving behaviors by frequency during that same timeframe, along with their relative, correlative collision risk:

Top 10 observed driving behavior (in order of frequency)	Correlative Collision Risk	2017-2018 Frequency
Driver not wearing seatbelt	4	Declining
Late response	5	Declining
Following distance >1 second to <2 seconds	25	Increasing
Smoking	35	Declining
Following distance >2 seconds to <3 seconds	34	Declining
Posted speed violation	17	Increasing
Food/drink observed	32	Declining
Cell Handheld observed	20	Declining
Other violation*	14	Increasing
Following distance <1 second	27	Declining

*Other violation examples include: traveling over the centerline, blocking traffic in an intersection or driving on the shoulder.

“The driving behavioral improvements we’re seeing are largely the result of our clients’ strong focus on

driver coaching and training.” Said Dr. Lisk, Vice President of Safety Services at Lytx, “Identifying risky driving behaviors and delivering that information in a format that is concise, intuitive and easy for fleets to understand and act on is key. Based on the data, we’re confident our clients are doing just that, and as a result are making the roadways safer for all.”

Risk in the Cab

With exponentially more human-reviewed data than any other video telematics provider, Lytx is able to identify real correlations between specific risky driving behaviors and the likelihood of those behaviors resulting in a collision. Here are the top ten driving behaviors correlated to a driver experiencing a collision in the next 90 days:

1. Collision
2. Blank stare
3. Drowsy driving
4. Driver not wearing seatbelt
5. Late response
6. Failed to keep an out**
7. Near collision
8. Near collision (unavoidable)
9. Aggressive driving
10. Falling asleep

**Failed to keep an out means the driver cut it unnecessarily close to another vehicle, person or object.

“Behind the wheel, even risky behaviors that may seem limited to just the driver—such as not wearing a seatbelt—can have real, quantifiable correlations to getting involved in a collision that can result in serious injury, loss of life and damage to an individual and company’s reputation and equipment,” said Lisk. “Insight into the relationship between risky driving behaviors and getting into a collision are invaluable for the trucking industry to consider as they prioritize and focus coaching efforts on the behaviors that will have the most impact in reducing collisions and improving overall safety within their fleet.”

Riskiest Roads

Lytx trucking-industry data shows the top five riskiest road segments for North American truck drivers between January and September 2018 were:

1. Pennsylvania Route 309: Near Vera Cruz Road, Upper Saucon Township, (South of Allentown)
2. Pennsylvania Route 309: Near W. Emmaus Avenue, Allentown (Southeast of Queen City Municipal Airport)
3. Pennsylvania Route 181: Near Crooked Hill Road, Susquehanna Township (East of Harrisburg Area Community College)
4. Tennessee Interstate 40: Near Green Hill Road, Dandridge (East of Knoxville)
5. Tennessee Interstate 24: Near Belvoir Avenue, Chattanooga (Southwest of Chattanooga Metropolitan Airport)

“The ability to determine the level of risk posed by other vehicles on the road, beyond just other large trucks, is a degree of insight only Lytx can provide,” said Ryan Brandos, a Lytx data analyst, who presented the findings at ATA MC&E. “With this level of detail, managers and coaches can consider areas of concentrated risk so they can make informed decisions about the best routes for their drivers.”

These five road segments are 172 times more risky on average than the rest of Lytx’s trucking-industry footprint, based on Lytx’s proprietary risk score system. Four out of the five segments are near interchanges and the other is near an exit/on ramp, which are areas of high driver volatility. Rapid changes in driving speed and sudden lane changes to make exits/connections not only lead to more triggered events, but also amplify the risk posed by risky driving behaviors, as these volatile areas necessitate a greater amount of proactive and reactive driving.

Interestingly, the No. 1 and 2 riskiest segments only had two other road segments in between them. These two segments were substantially safer, as the 103rd and 811th riskiest across Lytx’s entire trucking-industry footprint and were both less than one-fourth as risky as the riskiest segment. The ability to provide insights into not only the riskiest segments along routes, but also potentially less risky alternatives are insights that only Lytx’s one-of-a-kind data set can provide.

Riskiest Times

Lytix trucking-industry data shows top riskiest days of the week and times of day for North American truck drivers between January and September 2018 were:

1. Day of the week with most collisions: Wednesday (peak between 2:00 – 4:00 a.m.)
2. Time of day with most collisions: Overnight (11:00 p.m. – 5:00 a.m.)
3. Day of week with most near collisions: Friday
4. Time of day with most near collisions: Afternoon (1:00 p.m. – 5:00 p.m.)
5. Day of week with least collisions: Monday

“There is a distinct difference between collision and near-collision trends,” said Brandos. “Collisions occur more frequently at night. We see those same drivers avoid contact during the afternoon hours, resulting in more near collisions during the day.”

About Lytx

At Lytx® we harness the power of video to transform fleets with improved safety, efficiency, productivity and profitability. Our flagship service, the Lytx DriveCam® safety program, sets the standard for driver safety in the industries we serve. The Lytx Video Services™ enhancement delivers a highly configurable user interface to provide fleet managers unparalleled visibility into their fleet operations, both in the moment and up to a week later. RAIR® Compliance Services helps DOT-regulated fleets comply with safety regulations, complementing the DriveCam Program. Lytx ActiveVision® service helps fleets detect and address distracted and drowsy driving, both in real time and over time, and additional services offer virtually limitless solutions for fleets and field operations of any profile. We protect more than 3,000 commercial and government fleet clients worldwide who drive billions of miles each year. For more information, visit www.lytx.com, @lytx on Twitter, or our [Facebook](#) page or [YouTube](#) channel.

SHARE



MEDIA INQUIRIES

corpcomm@lytx.com

[← Back to all news](#)

Subscribe to our newsletter

Our Best Fleet Forward newsletter delivers monthly insights on fleet management.

Get started today.

[1-866-419-5861](tel:1-866-419-5861) [Contact Us](#) [Book a Demo](#)

SOLUTIONS

[Fleet Management Overview](#)
[Fleet Dash Cams](#)
[Fleet Safety](#)
[Fleet Tracking](#)
[DOT Compliance](#)
[ELD Compliance](#)
[FedEx VEDR](#)
[Lytx Integration Network](#)

GUIDES

[ADAS](#)
[CSA Scores](#)
[Defensive Driving for Commercial Fleets](#)
[Distracted Driving](#)
[DOT Regulations](#)
[ELD Guide](#)
[Fleet Maintenance](#)
[Fleet Management App](#)
[Fleet Management Solutions](#)
[Fleet Risk Management](#)
[Fuel Management Systems](#)

FEATURES

[DriveCam Event Recorder](#)
[Lytx Driver App](#)
[Machine Vision and Artificial Intelligence](#)
[Risk ID Without Recording](#)
[Continual Behavior Reporting](#)
[Preventative Maintenance](#)
[Diagnostic Trouble Codes](#)

ABOUT US

[Our Story](#)
[Our Technology](#)
[Our Team](#)
[Careers](#)
[News and Events](#)
[Who We Serve](#)
[Success Stories](#)

SUPPORT & LOGIN

[Support](#)
[Lytx Account Login](#)
[Lytx Compliance Services \(RAIR\) Portal](#)
[Lytx DriveCam Academy](#)
[Parts Store](#)

RESOURCES

[Blog](#)
[Buyer's Guide to Video Telematics](#)
[The Fleet Podcast](#)
[Videos](#)
[All Resources](#)

#1226

Solutions for Fleet and Driving
Telematics Systems

SITES

English (U.S.A.)
English (U.K.)



¹WARNING — The Lytx Event Recorder is a driver aid only. Never wait for the device to provide a warning before taking measures to avoid an accident. ²Estimated cost.
³Limited time offer. That services are provided at no cost for up to 3 months. Fees for shipping of hardware may apply.
⁴Subject to available cellular network coverage.
⁵Estimate based upon select sampling of Lytx client data.
© Copyright Lytx, Inc. 2021. All rights reserved.

[Site Map](#) [Legal](#) [Terms](#) [Privacy](#) [Driver Info](#)

