

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

CESAR PADILLA, individually and on	)	
behalf of all others similarly situated,	)	
	)	Case No. _____
Plaintiff,	)	
	)	CLASS ACTION COMPLAINT
v.	)	
	)	JURY TRIAL DEMANDED
SPACEXAI CORP., f/k/a X.AI CORP., a	)	
Nevada corporation; and SPACEXAI LLC,	)	INJUNCTIVE RELIEF DEMANDED
f/k/a X.AI LLC, a Nevada limited	)	
liability company,	)	
	)	
Defendants.	)	

CLASS ACTION COMPLAINT

Plaintiff Cesar Padilla, on behalf of himself and all other similarly situated individuals (“Plaintiff”), by and through Plaintiff’s attorneys, brings this Class Action Complaint against Defendants SPACEXAI CORP., formerly known as X.AI CORP., and SPACEXAI LLC, formerly known as X.AI LLC (collectively, “xAI” or “Defendants”). Plaintiff’s allegations are based on personal knowledge as to Plaintiff, on the investigation of counsel as to publicly observable functionality, and on information and belief as to matters concerning Defendants’ proprietary systems and practices within Defendants’ knowledge, which will be subject to discovery.

INTRODUCTION

1. Every individual has unique biometric identifiers by which he or she can be identified. One such biometric identifier is a person’s facial geometry.

2. As the Illinois General Assembly has found: “[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically

unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.” 740 ILCS § 14/5(c).

3. Pursuant to Illinois’ Biometric Information Privacy Act (“BIPA”), 740 ILCS § 14/1, *et seq.*, Illinois prohibits, among other things, private entities from collecting, capturing, obtaining, disclosing, redisclosing, disseminating or profiting from the biometric identifiers or information of an individual without providing written notice and without obtaining a written release from the impacted individual or his authorized representative. BIPA also requires private entities in possession of biometric identifiers to adopt retention and destruction policies and to take measures to prevent the release of that information.

4. In violation of BIPA, at relevant times, Defendants — the developers and operators of the generative artificial-intelligence service marketed as “Grok” — collected, captured, and otherwise obtained the facial geometric scans of thousands of Illinois citizens in violation of BIPA. Specifically, and as confirmed by Grok’s observable functionality, when a Grok user uploads a photograph depicting a human face and asks Grok to analyze, rate, edit, transform, or generate content based on that face, Defendants’ systems locate the face, examine the configuration of its features, and create and use a face-specific representation that measures, maps, or otherwise encodes the geometry of that face — including, on request, the proportions, symmetry, angles, and spatial relationships among the eyes, nose, lips, jaw, and facial contour. Defendants possessed the biometric identifiers and information without having adopted or made public any policy, written or otherwise, to govern the retention and destruction thereof.

5. This case does not allege that a photograph, standing alone, is a biometric identifier under BIPA. Photographs themselves are excluded from BIPA’s definition of a biometric

identifier. The challenged conduct is different: when Grok performs face-specific analysis or identity-preserving image manipulation, Defendants collect, capture, derive, or otherwise obtain a scan of face geometry and/or biometric information, separate from the underlying photograph.

6. Defendants engaged in the above-described conduct: (a) without informing the impacted individuals, including Plaintiff and members of the proposed class (the “Class” and the members thereof, “Class Members”) that their biometric identifiers were being collected, captured, and otherwise obtained; (b) without informing the impacted individuals in writing of the specific purpose and length of term of the collection, capture, and obtainment of the biometric identifiers and information; and (c) without seeking and obtaining written releases from such impacted individuals or their authorized representatives.

7. As the Illinois General Assembly has found and the Illinois Supreme Court has confirmed, the harm to Plaintiff and Class Members as a result of the BIPA violations alleged herein has already occurred.

8. Further, as businesses worldwide compete to develop ever more advanced artificial-intelligence and facial-analysis technology, the race for data imperils the privacy of individuals everywhere. Public policy in Illinois provides that given the risks of unwanted data collection and disclosure, its citizens need the power to make decisions about the fate of their unique biometric identifiers and information. Defendants’ actions robbed Plaintiff and Class Members of that power.

9. Moreover, as a direct result of Defendants’ actions, each individualized scan of a person’s facial geometry is generated within, and can be tied back to, the authenticated Grok account through which the originating photograph was uploaded, together with the account holder’s identifying information and conversation history. This, in turn, makes it possible to

connect the biometric identifiers and information of Plaintiff and Class Members that have been collected, captured, and otherwise obtained to the specific, identified individuals from whom they were taken, subjecting Plaintiff and Class Members to increased surveillance, stalking, identity theft, social engineering (a type of hacking technique) and other invasions of privacy and fraud. In addition, as a direct result of Defendants' actions, Plaintiff's and Class Members' biometric identifiers and information are no longer under their control. These injuries, which are imminent and clearly impending, are in addition to the injuries Plaintiff and Class Members have already sustained as a result of Defendants' actions.

10. Plaintiff brings this Class Action Complaint seeking: (a) statutory damages of \$5,000 per BIPA violation, or, alternatively, if Defendants acted negligently, \$1,000 per BIPA violation, along with attorneys' fees and costs; (b) an injunction (i) barring Defendants from any further use of individuals' biometric identifiers and information; (ii) barring Defendants from continuing to collect, capture, obtain, and profit from Plaintiff's and Class Members' biometric identifiers and information without complying with BIPA; (iii) requiring Defendants to delete and destroy all biometric identifiers and information in their possession, custody and control; and (iv) requiring Defendants to develop and make publicly available a BIPA-compliant retention schedule and destruction policy; and (c) other relief as alleged herein.

PARTIES

11. At all relevant times, Plaintiff Cesar Padilla was and remains an Illinois resident and citizen residing in Worth, Cook County, Illinois. Defendants performed facial geometric scans of Plaintiff from photographs Plaintiff uploaded to Grok while physically located in Illinois.

12. Defendant SpaceXAI LLC, formerly known as X.AI LLC and acquired by Space Exploration Technologies Corp. ("SpaceX") in February 2026, is a limited liability company

organized under the laws of Nevada that conducts substantial business throughout Illinois, including in Cook County. SpaceXAI LLC is the entity identified in the Grok Terms of Service and Privacy Policy as the party with which Grok users contract and as the entity responsible for the personal information Grok collects. On information and belief, SpaceXAI LLC is a wholly owned subsidiary of Defendant SpaceXAI Corp. SpaceXAI LLC (under its former name, X.AI LLC) is registered with the Illinois Secretary of State to transact business in Illinois, including in Cook County.

13. Defendant SpaceXAI Corp., formerly known as X.AI Corp. prior to its February 2026 acquisition by SpaceX, is a Nevada corporation that conducts substantial business throughout Illinois, including in Cook County. On or about August 13, 2026, the corporation changed its name from X.AI Corp. to SpaceXAI Corp. On information and belief, SpaceXAI Corp. was, until February 2, 2026, a wholly owned subsidiary of X.AI Holdings Corp., which on that date merged into and became part of SpaceX. SpaceXAI Corp. is now, on information and belief, a wholly owned subsidiary of SpaceX. SpaceXAI Corp. manages and controls the operations of SpaceXAI LLC.

14. On or about August 13, 2026, following SpaceX's acquisition of the xAI business and the public rebranding of that business as "SpaceXAI," X.AI Corp. and X.AI LLC rebranded to SpaceXAI Corp. and SpaceXAI LLC, respectively. As of the date of this Complaint, Defendants publish the Grok Terms of Service, Privacy Policy, and Acceptable Use Policy under the name "SpaceXAI" at the x.ai domain. Documents, policies, and public statements issued under the names "xAI," "X.AI Corp.," and "X.AI LLC" during the Class Period were issued by the Defendants named herein under their former names. To the extent the Grok business has been

transferred to or is operated by any successor or affiliate entity, Plaintiff intends to amend this Complaint to name that entity.

15. Defendants together own, control, and operate an artificial-intelligence model and product named Grok, including its image-understanding, image-analysis, image-editing, and image-generation features. On information and belief, Defendants co-developed the Grok family of artificial-intelligence models at issue here; operate as a single, integrated enterprise with respect to the development, operation, and monetization of Grok; share common ownership, officers, and management; and each participated in, directed, authorized, or controlled the conduct alleged herein. Each Defendant is a “private entity” within the meaning of 740 ILCS § 14/10.

JURISDICTION AND VENUE

16. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(d)(2) (the “Class Action Fairness Act”) because at least one member of the Class is a citizen of a State different from at least one Defendant, the aggregate amount in controversy exceeds \$5,000,000, exclusive of interest and costs, and there are 100 or more members of the Class. Plaintiff is a citizen of Illinois. No Defendant is a citizen of Illinois. Defendants are organized under the laws of Nevada and maintain principal places of business in Texas and/or California. *See* 28 U.S.C. § 1332(c)(1), (d)(10). Because it is estimated that the Class will have thousands of members and Defendants’ intentional and reckless violations of BIPA are punishable by statutory damages of \$5,000 per violation, the amount in controversy is well in excess of \$5,000,000. To the extent any claim asserted herein falls outside the Court’s original jurisdiction, this Court has supplemental jurisdiction over that claim pursuant to 28 U.S.C. § 1367(a).

17. Plaintiff and Class Members have Article III standing. Defendants’ collection, capture, and retention of their biometric identifiers without the notice and written release BIPA

requires deprived them of the opportunity to consider whether, and on what terms, to permit Defendants to obtain their biometric data, and stripped them of control over their immutable biometric identifiers. That deprivation is a concrete, particularized injury that bears a close relationship to harms traditionally recognized at common law, including intrusion upon seclusion. Defendants' unlawful retention of Plaintiff's and Class Members' biometric identifiers, and their failure to develop, publicly disclose, and comply with a retention schedule and destruction guidelines, likewise inflicts a concrete privacy injury.

18. This Court has personal jurisdiction over Defendants because Defendants purposefully direct Grok to, and transact business with, Illinois residents; accept and process photographs and prompts transmitted from Illinois; return Grok's outputs to users located in Illinois; sell paid Grok subscriptions to Illinois residents; and X.AI LLC is registered to transact business in Illinois. Defendants collected, captured, and otherwise obtained biometric identifiers and information derived directly from photographs that were created in Illinois, uploaded from Illinois, and managed via Illinois-based user accounts, computers, and mobile devices, and thereby exposed residents of Illinois to ongoing privacy risks within Illinois. Defendants knew or had reason to know that collecting, capturing, and obtaining Illinois citizens' and residents' biometric identifiers and information without providing the requisite notice or obtaining the requisite releases would deprive Illinois citizens and residents of their statutorily-protected privacy rights, neutralize Illinois citizens' and residents' ability to control access to their biometric identifiers and information via their Illinois-managed devices, and expose Illinois citizens and residents to potential surveillance and other privacy harms as they went about their lives within the state. Plaintiff's claims arise directly out of these Illinois-directed contacts.

19. Plaintiff's own BIPA transactions occurred primarily and substantially in Illinois. Plaintiff was physically located in Illinois when Plaintiff accessed Grok, uploaded the relevant photograph(s), transmitted the relevant prompts, and received Grok's face-specific analysis and/or edited outputs. Unlike a dataset assembled by third parties and later obtained by a defendant, the challenged collection here occurs in a direct, real-time transaction between the Illinois user and Defendants: the Illinois user transmits the photograph to Defendants, Defendants process it and return the output to the Illinois user, and the privacy injury caused by Defendants' failure to obtain BIPA-compliant consent is suffered in Illinois.

20. Venue is proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the acts or omissions giving rise to the claims alleged herein occurred in this District. Alternatively, venue is proper under 28 U.S.C. § 1391(b)(3) because this Court has personal jurisdiction over Defendants.

ILLINOIS BIOMETRIC PRIVACY LAWS

21. BIPA seeks to safeguard individuals' biometric identifiers and information.

22. Biometric identifiers include a scan of an individual's face geometry. 740 ILCS § 14/10. Although photographs themselves are excluded from the definition of "biometric identifier," BIPA separately protects face-geometry data extracted or created from a photograph. *See id.*

23. Biometric information is "any information . . . based on an individual's biometric identifier used to identify an individual." 740 ILCS § 14/10.

24. Pursuant to BIPA, a private entity, such as Defendants, is among other things: (a) prohibited from collecting, capturing or otherwise obtaining an individual's biometric identifiers and information without providing written notice and obtaining a written release; (b) prohibited

from selling, leasing, trading or otherwise profiting from an individual's biometric identifiers and information; (c) prohibited from disclosing, redisclosing or otherwise disseminating an individual's biometric identifiers or information in the absence of circumstances specifically set forth in the statute; and (d) required, to the extent it is in possession of biometric identifiers or information, to develop a written policy, made available to the public, that establishes a retention schedule and guidelines for permanently destroying such identifiers and information. 740 ILCS § 14/15.

25. BIPA provides for a private right of action and allows a prevailing party to recover liquidated damages in the amount of: (a) \$1,000 or actual damages, whichever is greater, for negligent violations of its provisions; and (b) \$5,000 or actual damages, whichever is greater, for intentional or reckless violations of its provisions. 740 ILCS § 14/20. BIPA also allows for the recovery of attorneys' fees and costs and injunctive relief. 740 ILCS § 14/20.

ALLEGATIONS

I. Allegations Related to Plaintiff

26. Plaintiff is an Illinois resident and an authenticated Grok user. Plaintiff's Grok account is associated with identifying account information, including his full name, email address, and other profile information.

27. Within the past year, while physically located in Worth, Illinois and Chicago, Illinois, Plaintiff accessed Grok using the Grok mobile application from an Illinois-based internet connection and Plaintiff's authenticated account.

28. Plaintiff uploaded to Grok several photographs depicting Plaintiff's own face (the "Plaintiff Photos"). The Plaintiff Photos were taken in Illinois, stored on Plaintiff's mobile device

in Illinois, and were transmitted to Defendants' servers while Plaintiff was physically located in Illinois.

29. For example, Plaintiff uploaded to Grok a selfie of himself sitting in his car, which depicted his unobstructed face, and asked Grok to produce a professional headshot from his uploaded selfie.¹ In response, Grok generated a professional headshot of Plaintiff, processing and modifying his photograph, including his face, to do so, while preserving Plaintiff's recognizable facial features and unique identity. Plaintiff also uploaded other images of his face to Grok, asking Grok to make edits to his facial image. For example, Plaintiff uploaded another facial selfie to Grok, asking Grok to "change me into [N]aruto," which facial image Grok processed and modified, preserving Plaintiff's recognizable facial features and unique identity.

30. As is the case for all Class Members, Defendants have, upon information and belief, captured biometrics from the Plaintiff Photos by automatically locating and scanning Plaintiff's face, and by extracting geometric data relating to the contours of Plaintiff's face and the proportions of, and spatial relationships among, facial landmarks, such as Plaintiff's eyes, nose, mouth, jaw, and facial contours. Defendants then used this biometric information to generate the identity-preserving edited image that Grok returned to Plaintiff, as set forth more fully below.

31. The facial biometric data Defendants captured was capable of identifying Plaintiff because, upon information and belief, it was unique to Plaintiff's own facial features. Further, it was created and used within Plaintiff's authenticated account session, and Defendants possessed account information capable of linking the representation to Plaintiff's real-world identity.

¹ This facial image that Plaintiff uploaded is the same image Plaintiff uses for his profile picture on Grok.

32. Defendants: (a) never advised Plaintiff in writing or otherwise that they were performing scans of Plaintiff's facial geometry; (b) never informed Plaintiff in writing or otherwise of the specific purpose and length of term for which they were collecting, capturing, obtaining, storing, and using Plaintiff's biometric identifiers and information; and (c) never sought, nor received, a written release from Plaintiff or Plaintiff's authorized representative that allowed Defendants to collect, capture, or obtain Plaintiff's biometric identifiers and information.

33. Plaintiff never consented, agreed, or gave permission — written or otherwise — to Defendants for the collection or storage of Plaintiff's unique biometric identifiers or biometric information. Plaintiff requested edits to his facial image without any knowledge that Defendants used face-processing architecture to extract his biometric data.

34. Defendants possessed Plaintiff's biometric identifiers and information at least while processing the Plaintiff Photos and generating the edited image and, on information and belief, retained that data and the associated image-processing context beyond the instant of collection. Defendants did not make available to Plaintiff a written, BIPA-compliant retention schedule or destruction policy governing that data.

35. As alleged above, Defendants' conduct has injured Plaintiff and subjected Plaintiff to additional imminent and certainly impending injuries.

II. Defendants' Unlawful Conduct

A. Grok and Its Face-Processing Functionality

36. Grok is Defendants' family of multimodal artificial-intelligence models and consumer-facing services, capable of processing and generating text, images, audio, video, and code. Introduced publicly in 2023 and initially integrated into the X (formerly Twitter) platform, Grok is now available through the website grok.com, standalone Grok mobile applications for iOS

and Android, the X platform, and application programming interfaces (“APIs”) through which developers incorporate Grok’s capabilities into third-party applications.

37. Grok is a commercial product. Defendants sell paid subscription tiers, including “SuperGrok” and, through the X platform, “Premium” and “Premium+” subscriptions, that provide expanded access to Grok’s features, including its image features. Grok reportedly had approximately 117 million monthly active users worldwide as of March 2026.

38. Only signed-in users may upload photographs to Grok. Every photograph uploaded to Grok is transmitted over the internet to computer servers owned, operated, or controlled by Defendants, is processed there, and the resulting output is transmitted back to the user. No part of the challenged processing occurs on the user’s own device.

39. In October 2024, Defendants added image-understanding (“vision”) capabilities to Grok, allowing users to upload photographs and ask Grok questions about them. By March 2025, Defendants added the ability to edit uploaded photographs through natural-language prompts. In August 2025, Defendants launched “Grok Imagine,” an image- and video-generation product. In December 2025, Defendants added an “Edit Image” function to the X platform that allows any user to apply Grok’s image editing to any publicly posted image, including photographs of other people.

40. Defendants have described Grok’s image system, code-named “Aurora,” as “an autoregressive mixture-of-experts network trained to predict the next token from interleaved text and image data,” trained on “billions of examples from the internet.” Defendants state that Aurora has “native support for multimodal input, allowing it to take inspiration from or directly edit user-

provided images,” and advertise “Realistic portraits” and “Celebrities” among Aurora’s supported capabilities, together with the ability to render “precise visual details” of real-world subjects.²

41. Defendants have since released successor image and video models, including the Grok Imagine API (announced January 28, 2026), Grok Imagine “Quality Mode” (May 2026), and Grok Imagine 1.5 (June 3, 2026), an image-to-video model that Defendants describe as turning “a single still image into fluid, cinematic video” while staying faithful to the source image.

42. Defendants’ developer documentation for Grok’s image-understanding capability states that there is no limit on the number of images a user may submit, and contains no policy, restriction, or guidance of any kind concerning images of people or human faces.

B. Grok Scans, Measures, and Reports the Geometry of Faces in Uploaded Photographs

43. A common and widely documented use of Grok is the generation of so-called “aesthetic reports.” To generate these reports, a user uploads a photograph of a face and asks Grok to analyze and rate the depicted person’s facial structure, proportions, symmetry, and individual features.

44. In response, Grok returns a structured, feature-by-feature assessment of the face. In performing this analysis, Grok analyzes an uploaded close-up photograph of a face and generates a report capable of including, *inter alia*: an assessment of bone structure and framework, including the width and forward projection of the jawline, cheekbone prominence, midface breadth, and overall craniofacial structure; an assessment of symmetry; an assessment of proportions and harmony, including the “facial thirds” (hairline to brow, brow to nose base, nose base to chin), ramus height, and gonial angle, and observations based on same; an assessment of

²Grok Image Generation Release, xAI (Dec. 9, 2024), <https://x.ai/news/grok-image-generation-release>.

the eyes, including their canthal tilt; an assessment of the nose, including its dimensions; and an assessment of the lips and mouth, including vermilion show and the philtrum.

45. Grok's assessment utilizes the standard vocabulary of craniofacial anthropometry, which is the measurement of spatial relationships among anatomical landmarks on the human face. For example: the "facial thirds" are the vertical proportions of the face measured between the hairline, brow, base of the nose, and chin; the "gonial angle" is the angle formed by the mandible at the corner of the jaw; the "ramus height" is the vertical distance of the mandibular ramus from the uppermost point of the condyle down to the bottom corner of the jaw angle; the "canthal tilt" is the angle of the line connecting the inner and outer corners of the eye; the "nasal base" width is the distance between the outer edges of the nostrils; the "dorsum projection" describes the profile of the bridge of the nose; and facial "symmetry" is a comparison of the positions and dimensions of paired features on the left and right sides of the face. Each is a measurement of face geometry.

46. Grok cannot report a person's gonial angle without having located the corner of that person's jaw and computed its angle. Likewise, it cannot report a person's facial thirds without having located that person's hairline, brow, nose base, and chin and computed the distances between them. Nor can it assess symmetry without having located paired features and compared their positions. Grok's output is therefore direct evidence that, in the course of generating its facial assessment, Defendants' systems scanned the geometry of the depicted face.

47. Grok itself has described its face analysis to users in these terms, confirming that its measurements of specific facial geometry are not mere coincidence. For example, Grok itself explains that, when it analyzes a face for these purposes, it directly sees the uploaded image. According to Grok, it does not guess, but rather processes the pixels with a well-trained visual system, drawing on training in facial anatomy and anthropometry, including facial thirds and phi

ratios. Grok has further explained that it performs a systematic breakdown consisting of, *inter alia*, bone structure and projection, vertical and horizontal proportions, symmetry analysis, and feature-by-feature evaluation (eyes, nose, jaw, lips, etc.). After performing such analysis, Grok is capable of providing the technical version of that analysis with specific measurements it can estimate from the photo.

48. Grok also performs targeted edits and transformations of uploaded photographs while preserving the depicted person's recognizable identity. For example, Grok can change a person's facial expression, add or remove facial hair, alter apparent age, or place the person in a different scene, while keeping the person recognizably the same. Grok has described this functionality to users as a "sophisticated generative edit that understands facial anatomy and muscle movements," in which "[t]he model keeps the person's identity . . . as consistent as possible while only altering" the requested attributes.

49. A system that changes individual facial attributes while keeping the person recognizably the same must distinguish the subject from the surrounding image, localize the face, and carry forward through the transformation the unique, identity-bearing structure of that particular face — the shape and relative positions of the eyes, nose, mouth, jaw, and facial contour — sufficient to re-render that specific individual's face in the output. A representation sufficient to reproduce a recognizable rendering of a particular individual's face is, by its nature, a representation of that individual's face geometry that is capable of distinguishing that individual from others.

50. Defendants' own marketing confirms that Grok's image models encode identity-bearing facial characteristics of specific individuals. Defendants advertise "Celebrities" as a

supported use case, and when prompted to generate images of recognizable public figures, Grok produces outputs in which the person remains readily identifiable based on facial appearance.

51. When making alterations to a facial image, as discussed above, Grok confirmed that it references the original image the user uploaded using its unique ID. On information and belief, uploaded photographs and the face-specific data derived from them are stored on Defendants' servers under persistent identifiers and remain available to Defendants' systems across multiple turns of a conversation and within the user's stored conversation history.

52. Defendants' Privacy Policy confirms that Grok conversations, including uploaded images, are retained by default. It describes a separate "Private Chat" mode in which conversations are deleted within 30 days — which indicates that conversations outside that mode, including the images and outputs they contain, are retained for longer than 30 days. The Privacy Policy further provides that Defendants use personal information, including User Content such as "images," "to train our models," and the Terms of Service provide that a user "can select whether or not" Defendants use the user's User Content "to improve our products and services and train our models."³

53. The precise internal architecture Defendants use to perform these functions is proprietary and within Defendants' exclusive knowledge. Unlike other developers of comparable artificial-intelligence systems, Defendants have published no description of how Grok processes images of people. Defendants' published model cards for Grok 4, Grok 4 Fast, Grok 4.1, and Grok 4.20, for instance, do not contain any description of the image-processing architecture or evaluation of any safeguard relating to faces or the identification of individuals.

³ SpaceXAI, *Privacy Policy* §§ 2, 3, 5 (eff. Aug. 24, 2026), <https://x.ai/legal/privacy-policy>; SpaceXAI, *Consumer Terms of Service* § 4 (updated Sept. 11, 2026), <https://x.ai/legal/terms-of-service>.

54. Whether Defendants’ systems compute an explicit set of facial landmarks and the distances and angles among them, or, as is common in modern multimodal artificial-intelligence models, convert the region of the image containing the face into a high-dimensional numerical representation from which the structure of the face and the identity of the depicted person can be recovered — the result is the same: in order to report facial proportions, angles, and symmetry, and in order to re-render a specific person’s face, Defendants’ systems create, capture, obtain, and use a face-specific digital representation that measures, maps, or otherwise encodes the geometry of the depicted face. Published, peer-reviewed research confirms that general-purpose multimodal artificial-intelligence models of the kind Defendants deploy encode identity-distinguishing facial information: such a model has previously been shown, with no face-specific training, to determine whether two photographs depict the same person at accuracy comparable to or exceeding that of human examiners.⁴

55. This internal representation is separate from the photograph itself. Plaintiff does not seek relief based merely on Defendants’ receipt of an ordinary photograph. Plaintiff challenges Defendants’ extraction, creation, capture, collection, possession, and use of the face-specific biometric representation derived from the photograph.

56. Unlike technology that merely creates a whole-image hash to determine whether two image files are duplicates, Grok’s challenged functionality is directed to the human face itself. Grok locates the face, measures and reports its proportions, angles, and symmetry, performs targeted facial edits, and preserves a particular person’s recognizable identity across transformed outputs.

⁴ See, e.g., Robin S.S. Kramer, *Face to Face: Comparing ChatGPT with Human Performance on Face Matching*, 54 *Perception* 65, 65–67 (2025), <https://doi.org/10.1177/03010066241295992>.

57. Moreover, on information and belief, when presented with two photographs, Grok can also determine whether they depict the same individual, further demonstrating that the facial data Grok processes is sufficient to identify and track a specific person.

C. Grok’s Facial Representations Are Capable of Identifying Plaintiff and Class Members

58. The biometric data Grok collects is capable of identifying the person from whom it is collected.

59. For users who sign into Grok through X, Defendants receive account-linked information such as a profile image, username, numeric account identifier, date of birth, and Grok conversation history. For users who sign in through grok.com or the Grok mobile applications, Defendants collect the user’s name, contact information, account credentials, and date of birth, together with payment information for paid subscriptions and technical data including the user’s IP address and device type.

60. When an authenticated user uploads a photograph of himself or herself and expressly identifies the depicted person as “me,” “my face,” or the account holder, Defendants can connect the face-specific representation derived from the image to the identified account without any need to discover the subject’s identity from scratch.

61. Independently, the geometric representation Grok creates of a person’s face — the proportions, angles, and symmetry of that person’s features and the identity-bearing structure Grok preserves through its edits — is intrinsically unique to that person and is itself capable of being used to identify him or her, alone or in combination with other information available to Defendants.

62. On information and belief, Defendants use or can use the facial representation to maintain identity consistency within a chat or image-editing workflow, to distinguish the depicted

person from others, to locate the person's face within an image, and to preserve the same person's recognizable identity across generated or edited outputs.

D. Defendants Know How to Obtain Written Releases for Facial Data — But Do Not Do So for Grok Users

63. Public reporting concerning an internal xAI initiative known as “Project Skippy” demonstrates both that Grok was trained on facial biometric data and that Defendants are familiar with facial-data collection and consent procedures. According to that reporting, in 2025 Defendants asked employees designated as “AI tutors” to have their faces recorded during conversations to train Grok and Grok-related products on their facial expressions. Defendants asked those employees to execute release forms granting Defendants perpetual, worldwide rights to use, reproduce, and distribute their faces and voices. Employees who objected were reportedly told that participation was a job requirement tied to xAI's mission.⁵

64. Project Skippy demonstrates, at minimum, that Defendants trained Grok on human facial expressions, understand the distinction between ordinary audiovisual material and specifically collected facial data, regard facial data as valuable for developing Grok, and that Defendants know how to obtain written releases for facial data when they choose to do so.

65. Despite this, Defendants do not provide Grok users with a BIPA-compliant written disclosure before Grok performs the challenged facial processing. Defendants do not tell users that Grok will create, capture, collect, or otherwise obtain a scan of face geometry or biometric information from an uploaded photograph; do not state the specific purpose and length of term for which such biometric data will be collected, stored, and used; and do not obtain a written release

⁵ See Victor Tangermann, *Leaked Documents Show xAI Employees Were Alarmed by Something They Were Asked to Do at Elon Musk's AI Startup*, Futurism (July 22, 2025), <https://futurism.com/leaked-documents-xai-employees-alarmed> (reporting on Business Insider's account of Project Skippy).

from the subject before collection. Nor did Plaintiff or any Class Member execute a written release by creating a Grok account or by accepting Defendants' Terms of Service or Privacy Policy. Neither document discloses that Defendants collect, capture, or otherwise obtain biometric identifiers or biometric information, much less the specific purpose and length of term of any such collection, and a user cannot give "informed written consent" — by electronic signature or otherwise — to a practice that has never been disclosed to him or her. *See* 740 ILCS § 14/10 (defining "written release").

66. Defendants' public Privacy Policy does not cure that failure. The Privacy Policy makes no mention of "face," "facial," "face geometry," "biometric identifier," or "biometric information," nor does it contain any retention schedule or destruction guideline for biometric data or mechanism for obtaining a written release. The closest Defendants come is a statement that they "do not aim to collect sensitive personal information (ex., information related to racial or ethnic origin, political opinions, religion or other beliefs, health, biometric scans, criminal background, or trade union membership) and ask that you do not provide us with any such information." This language, however, does nothing to disclaim Grok's capture and use of biometric data from each uploaded face that it processes, as alleged herein. To the contrary, by identifying "biometric scans" as "sensitive personal information," Defendants acknowledge that they understand the sensitivity of such data — yet they designed and market Grok to locate, measure, and re-render the faces in users' photographs without providing the notice or obtaining the release BIPA requires. Nor does the Privacy Policy's statement that, "in relation to Grok's training," no "uploaded image [is] used for identification purposes" change the analysis. That

statement appears in a sentence expressly addressing Grok's training; it says nothing about the face-specific processing Grok performs in response to user prompts.⁶

67. In further violation of BIPA, as private entities in possession of Plaintiff's and Class Members' biometric identifiers and information, Defendants failed to adopt or make available to the public a retention schedule or guidelines for permanently destroying such biometric identifiers and information once the initial purpose for collecting them had or has been satisfied.

68. In further violation of BIPA, on information and belief, Defendants profited from the biometric identifiers and information of Plaintiff and Class Members. Defendants sell paid subscriptions that provide access to the very image-analysis and image-editing features through which the biometric identifiers are captured, and Defendants' Privacy Policy and Terms of Service provide that User Content, including uploaded images, is used to train and improve Defendants' commercial models unless the user opts out.

69. Defendants' violations of BIPA were intentional and reckless or, in the alternative, negligent. Defendants were aware of the sensitivity of facial biometric data and of the need for consent to collect it: their own Privacy Policy identifies "biometric scans" as sensitive personal information, and, in connection with Project Skippy, Defendants sought written releases from their own employees before collecting their facial data. Defendants nonetheless chose to collect, capture, and otherwise obtain Grok users' face geometry without providing any notice or obtaining any release.

⁶ SpaceXAI, *Privacy Policy* § 2 (eff. Aug. 24, 2026), <https://x.ai/legal/privacy-policy>.

III. Plaintiff's and Class Members' Injuries and Damages

70. As alleged herein, as a result of Defendants' unlawful conduct, Plaintiff and Class Members have already sustained injuries and face many more imminent and certainly impending injuries, which injuries they will continue to suffer.

71. Defendants' unlawful conduct has resulted in, among other things: (a) Plaintiff's and Class Members' unique biometric identifiers and information being collected, captured, and otherwise obtained without the requisite notice having been given and without the requisite releases having been obtained; and (b) Plaintiff and Class Members being deprived of the very control over their biometric identifiers and information that BIPA was designed to protect.

72. To this day, Plaintiff and Class Members do not know whether, where, or for how long Defendants have retained their biometric identifiers and information, whether that data has been used to train Defendants' models, or which individuals or entities have received, obtained, accessed, or otherwise made use of it, exposing them to the imminent and certainly impending injuries of identity theft, fraud, stalking, surveillance, social engineering and other invasions of privacy.

73. As a result of Defendants' misconduct, Plaintiff and Class Members have no recourse for the fact that their biologically unique information has been compromised. Moreover, Plaintiff and Class Members are likely to withdraw from biometric-facilitated transactions and other facially-mediated electronic participation.

CLASS ACTION ALLEGATIONS

74. Plaintiff brings this action on behalf of himself and as a class action under Federal Rule of Civil Procedure 23, seeking damages and equitable relief on behalf of the following Class for which Plaintiff seeks certification:

All Illinois residents who, while located in Illinois and logged into an authenticated Grok account, uploaded to Grok a photograph depicting their own face and used Grok to analyze, rate, edit, transform, or generate content based on that face, during the Class Period.

75. Excluded from the Class are: (a) Defendants; (b) any parent, affiliate or subsidiary of Defendants; (c) any entity in which Defendants have a controlling interest; (d) any of Defendants' officers or directors; (e) any successor or assign of Defendants; and (f) any person who executed a BIPA-compliant written release before the challenged collection. Also excluded are any judge or court personnel assigned to this case and members of their immediate families.

76. The "Class Period" begins on the date Defendants first made available to Illinois users Grok functionality that accepts and processes user-uploaded photographs — which, on information and belief, occurred in or about October 2024 — and continues through the date of class certification.

77. Plaintiff reserves the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery.

78. **Numerosity.** While the exact number of Class Members is not known at this time, Grok reportedly has approximately 117 million monthly active users worldwide, a substantial number of whom reside in Illinois, and Grok's image-analysis and image-editing functionality has been widely used. Plaintiff estimates the total number of Class Members to be in the thousands. Consistent with Rule 23(a)(1), the proposed Class is therefore so numerous that joinder of all members is impracticable. Class Members may be identified through objective means, including objective data available to Defendants regarding authenticated account records, account-profile

data, IP address and geolocation records, uploaded-image logs, prompt and conversation logs, and feature-use records. Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, social media and/or published notice.

79. **Commonality and predominance.** Common questions of law and fact exist as to all Class Members. These common questions of law or fact predominate over any questions affecting only individual members of the proposed Class. Common questions include, but are not limited to, the following:

- a. Whether Grok's challenged face-specific functionality detects and processes facial geometry;
- b. Whether Defendants collected, captured and otherwise obtained the biometric identifiers and information of Plaintiff and Class Members;
- c. Whether Defendants possessed the biometric identifiers and information of Plaintiff and Class Members;
- d. Whether the facial representations Defendants create are capable of identifying Plaintiff and Class Members;
- e. Whether Defendants profited from the biometric identifiers and information of Plaintiff and Class Members;
- f. Whether Defendants provided the notice required by BIPA before collecting, capturing, and otherwise obtaining the biometric identifiers and information of Plaintiff and Class Members;
- g. Whether Defendants obtained written releases from Plaintiff and Class Members or their authorized representatives before collecting, capturing,

and otherwise obtaining the biometric identifiers and information of Plaintiff and Class Members;

- h. Whether Defendants had in place — and disclosed to the public — the written retention and destruction policies required by BIPA while in possession of Plaintiff's and Class Members' biometric identifiers and information;
- i. Whether Defendants' violations of BIPA were negligent, intentional, or reckless; and
- j. Whether Plaintiff and Class Members are entitled to damages, equitable relief, and other relief.

Moreover, based on Defendants' public statements and the uniform operation of Grok, there is no reason to believe Defendants treated any of the photographs on which Grok performed a facial geometric scan differently from any others in terms of: (a) the way in which Defendants obtained the photographs; (b) the biometric identifiers and information collected, captured and otherwise obtained therefrom; (c) Defendants' failure to provide the requisite disclosures to Plaintiff and Class Members or their authorized representatives; (d) Defendants' failure to obtain the requisite releases from Plaintiff and Class Members or their authorized representatives; or (e) the nonexistence of a written, publicly-available retention and destruction schedule. In short, whether Defendants violated BIPA's requirements is a question that can uniformly be answered for all Class Members, including Plaintiff.

80. **Typicality.** Plaintiff's claims are typical of the claims of the Class Plaintiff seeks to represent because Plaintiff and all members of the proposed Class have suffered similar injuries

as a result of the same practices alleged herein. Plaintiff has no interests to advance adverse to the interests of the other members of the proposed Class.

81. **Adequacy.** Plaintiff will fairly and adequately protect the interests of the proposed Class and has retained as counsel attorneys experienced in class actions and complex litigation.

82. **Superiority.** A class action is superior to other available means for the fair and efficient adjudication of this dispute. The injury suffered by each Class Member, while meaningful on an individual basis, may not be of such magnitude as to make the prosecution of individual actions against Defendants economically feasible. Even if Class Members could afford individual litigation, those actions would put immeasurable strain on the court system. Moreover, individual litigation of the legal and factual issues of the case would increase the delay and expense to all parties and the court system. A class action, however, presents far fewer management difficulties and provides the benefit of a single adjudication, economy of scale and comprehensive supervision by a single court.

83. In the alternative, the proposed Class may be certified because:

- a. The prosecution of separate actions by each individual member of the proposed Class would create a risk of inconsistent adjudications, which could establish incompatible standards of conduct for Defendants;
- b. The prosecution of individual actions could result in adjudications that as a practical matter would be dispositive of the interests of non-party Class Members or which would substantially impair their ability to protect their interests; and

- c. Defendants acted or refused to act on grounds generally applicable to the proposed Class, thereby making final and injunctive relief appropriate with respect to members of the proposed Class.

84. Pursuant to Rule 23(c)(4), particular issues are appropriate for certification — namely the common questions described above — because resolution of such issues would advance the disposition of the matter and the parties’ interests therein.

CLAIMS FOR RELIEF

COUNT ONE **(VIOLATION OF BIPA – 740 ILCS § 14/15(a))**

85. Plaintiff restates and realleges all paragraphs of this Class Action Complaint as though fully set forth herein.

86. As alleged above, Defendants violated BIPA by possessing Plaintiff’s and Class Members’ biometric identifiers and information without developing a written policy that they made available to the public that established a retention schedule and guidelines for permanently destroying biometric identifiers and information.

87. Defendants further violated BIPA by failing to comply with any such retention schedule and destruction guidelines and, on information and belief, by retaining Plaintiff’s and Class Members’ biometric identifiers and information after the initial purpose for collecting them — the generation of the requested analysis or edited image — had been satisfied, including in stored conversation histories and, on information and belief, in data used to train Defendants’ models.

88. Defendants’ violations of BIPA were intentional and reckless or, pleaded in the alternative, negligent.

89. As a direct and proximate result of Defendants' violations of BIPA, Plaintiff and Class Members have suffered and will continue to suffer injury.

90. Plaintiff and Class Members seek as monetary relief the greater of \$5,000 or actual damages or, pleaded in the alternative, \$1,000 or actual damages.

91. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that their biometric identifiers and information can be viewed and used by unauthorized persons. Plaintiff and Class Members have no adequate remedy at law for their injuries in that a judgment for monetary damages will not end the misuse of Plaintiff's and Class Members' biometric identifiers and information.

92. Plaintiff and Class Members also seek injunctive relief and the reasonable attorneys' fees, costs and expenses relating to this action.

COUNT TWO
(VIOLATION OF BIPA – 740 ILCS § 14/15(b))

93. Plaintiff restates and realleges all paragraphs of this Class Action Complaint as though fully set forth herein.

94. As alleged above, Defendants violated BIPA by collecting, capturing, and otherwise obtaining individuals' biometric identifiers and information, including the biometric identifiers and information of Plaintiff and Class Members, without providing the requisite written information and without obtaining the requisite written releases.

95. Specifically, before collecting or otherwise obtaining Plaintiff's and Class Members' biometric identifiers and information, Defendants failed to inform them in writing that a biometric identifier or biometric information was being collected or stored, in violation of 740 ILCS § 14/15(b)(1); failed to inform them in writing of the specific purpose and length of term for

which their biometric identifiers or biometric information were being collected, stored, and used, in violation of 740 ILCS § 14/15(b)(2); and failed to receive a written release executed by them, in violation of 740 ILCS § 14/15(b)(3).

96. Defendants' violations of BIPA were intentional and reckless or, pleaded in the alternative, negligent.

97. As a direct and proximate result of Defendants' violations of BIPA, Plaintiff and Class Members have suffered and will continue to suffer injury.

98. Plaintiff and Class Members seek as monetary relief the greater of \$5,000 or actual damages or, pleaded in the alternative, \$1,000 or actual damages.

99. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that their biometric identifiers and information can be viewed and used by unauthorized persons. Plaintiff and Class Members have no adequate remedy at law for their injuries in that a judgment for monetary damages will not end the misuse of Plaintiff's and Class Members' biometric identifiers and information.

100. Plaintiff and Class Members also seek injunctive relief and the reasonable attorneys' fees, costs and expenses relating to this action.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Cesar Padilla, on behalf of himself and on behalf of the Class, respectfully seeks from the Court the following relief:

- a. Certification of the Class as requested herein;
- b. Appointment of Plaintiff as Class representative and Plaintiff's undersigned counsel as Class counsel;

- c. An award of damages for Plaintiff and members of the proposed Class, including liquidated damages of \$5,000 for each intentional or reckless violation of BIPA or, alternatively, \$1,000 for each negligent violation, pursuant to 740 ILCS § 14/20;
- d. An award of equitable, injunctive and declaratory relief for Plaintiff and members of the proposed Class, including an injunction (i) barring Defendants from any further use of individuals' biometric identifiers and information; (ii) barring Defendants from continuing to collect, capture, obtain, and profit from Plaintiff's and Class Members' biometric identifiers and information unless and until Defendants comply with BIPA; (iii) requiring Defendants to delete and destroy all biometric identifiers and information in their possession, custody and control; and (iv) requiring Defendants to develop and make publicly available a BIPA-compliant retention schedule and destruction policy;
- e. An award of pre-judgment and post-judgment interest for Plaintiff and members of the proposed Class, as permitted by law;
- f. An award for Plaintiff and members of the proposed Class of reasonable attorneys' fees and costs of suit, including expert witness fees; and
- g. An award for Plaintiff and members of the proposed Class of any further relief the Court deems proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial on all claims so triable.

Dated: October 7, 2026

Respectfully submitted,

By: /s/ Nicholas R. Lange

NICHOLAS R. LANGE

JONATHAN M. JAGHER

nlange@jjlmlaw.com

jjagher@jjlmlaw.com

JUSTICE JAGHER LONDON & MILLEN LLC

100 Tri-State International, Suite 128

Lincolnshire, IL 60069

Phone: (224) 632-4500

Counsel for Plaintiff and the Putative Class