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

CODY CLARK, *on behalf of himself and all others similarly situated,*

Plaintiff,

v.

MICROSOFT CORPORATION,

Defendant.

Case No.: 2022CH12396

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Cody Clark ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint for violations of the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1 *et seq.*, against Defendant Microsoft Corporation ("Defendant" or "Microsoft"). Plaintiff alleges as follows based on personal knowledge as to himself, on the investigation of his counsel, and on information and belief as to other matters, and demands trial by jury.

NATURE OF ACTION

A. BIPA.

1. Plaintiff brings this action for damages and other legal and equitable remedies resulting from the illegal actions of Defendant in collecting, storing, and using Plaintiff's and other similarly situated individuals' biometric identifiers[1] and biometric information[2] (referred to,

[1] A "biometric identifier" is any personal feature that is unique to an individual, including but not limited to fingerprints, iris scans, voiceprints, DNA, and "face geometry".

[2] "Biometric information" is any information that is captured, converted, stored, or shared based on a person's biometric identifier and used to identify an individual.

collectively, as "biometrics") without providing the requisite written notice, obtaining the requisite prior informed written consent, or providing the requisite data retention and destruction policies, in direct violation of BIPA.

2. The Illinois Legislature has found that "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5(c). "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." *Id.*

3. In recognition of these concerns over the security of individuals' biometrics, the Illinois Legislature enacted BIPA, which provides, *inter alia*, that private entities like Defendant may not obtain and/or possess an individual's biometrics unless they: (1) inform that person in writing that biometric identifiers or information will be collected or stored, *see* 740 ILCS 14/15(b); (2) inform that person in writing of the specific purpose and length of term for which such biometric identifiers or biometric information are being collected, stored, and used, *see id.*; and (3) receive a written release from the person for the collection of his or her biometric identifiers or information, *see id.*

4. Moreover, entities collecting biometric identifiers and biometric information must publish publicly available written retention schedules and guidelines for permanently destroying biometric identifiers and biometric information. *See* 740 ILCS 14/15(a).

5. Further, entities must store, transmit, and protect an individual's biometric identifiers and biometric information using the same standard of care as within the industry and

in a manner at least as protective as the means used to protect other confidential and sensitive information. *See* 740 14/15(e).

6. Finally, entities are expressly prohibited from selling, leasing, trading or otherwise profiting from the individual's biometrics. *See* 740 15/15(c).

B. Defendant's Biometric Collection Practices.

7. Defendant Microsoft purveys platforms called Microsoft Azure "Azure" and Azure Cognitive Services ("ACS"), which are, respectively, a public cloud (allowing users to, *inter alia*, build and deploy applications; store data; deliver software on demand; and analyze data using machine learning and artificial intelligence) and cloud-based artificial intelligence services that help developers build cognitive solutions (that can see, hear, speak, and analyze) into their applications.

8. One Microsoft client that interfaces with and/or integrates Azure and/or ACS is Brainshark, Inc. ("Brainshark"). Brainshark provides sales enablement and readiness solutions, including video-based coaching, that are accessed by salespeople.

9. Using Brainshark's software, a salesperson may (1) record a video of herself and upload it to Brainshark's platform as to then (2) receive feedback (generated automatically by Machine Analysis) regarding their elevator pitch, responses to common objections, and/or other efforts to refine their skills. This feedback includes "emotion analysis" and "personality insights" that are informed by an analysis of the salespeople's facial expressions.

10. In conducting this analysis, Brainshark (1) collects, captures, and/or otherwise obtains; (2) stores; and/or (3) makes use of such individuals' biometric identifiers (namely, scans of facial geometry) and biometric information.

11. As Brainshark's software interfaces with and/or integrates Azure and/or ACS, Defendant Microsoft also (1) collects, captures, and/or otherwise obtains; (2) stores; and/or (3) makes use of such individuals' biometric identifiers and biometric information.

12. Microsoft sells access to its Azure and/or ACS platforms to other clients ("Biometrics Products and/or Services that interface with and/or integrate Azure and/or ACS" or "BPSAA") that (1) collect, capture, and/or otherwise obtain; (2) store; and/or (3) make use of individuals' ("BPSAA subjects") biometric identifiers and biometric information.

13. By way of BPSAA, Defendant (1) collects, captures, and/or otherwise obtains; (2) stores; and/or (3) makes use of the biometric identifiers and biometric information from a multitude of BPSAA subjects.

14. Yet Defendant has failed to comply with the foregoing provisions of § 15(a) and § 15(b) of BIPA.

15. Defendant has not adequately informed individuals who have interacted (knowingly or not) with its Azure and/or ACS platforms, by way of BPSAA, that it collects and/or stores their biometric identifiers and/or biometric information.

16. Defendant has not adequately informed such individuals of the specific purpose and length of term for which their biometric identifiers and/or biometric information are collected, stored, and/or used.

17. Defendant has not obtained written consent from such individuals regarding its biometric practices.

18. And Defendant has not provided any data retention or destruction policies to such individuals.

19. If Defendant's collection of biometric identifiers and biometric information were to fall into the wrong hands, by data breach or otherwise, the individuals to whom these sensitive and immutable biometric identifiers and biometric information belong could have their identities stolen, among other serious issues.

20. Plaintiff brings this action to prevent Defendant from further violating the privacy rights of Illinois residents, and to recover statutory damages for Defendant's unauthorized collection, storage, and use of these individuals' biometrics in violation of BIPA.

PARTIES

21. Plaintiff Cody Clark is, and has been at all relevant times, a resident of Chicago, Illinois. He has an intent to remain there and is therefore domiciled in Illinois. Plaintiff Clark's biometric identifiers and/or biometric information were collected, captured, otherwise obtained, and/or stored by Defendant in or around August 2020 when Plaintiff Clark utilized – while he was located within the state of Illinois – the products and/or services of one of Defendant's clients (Brainshark) which interfaced with and/or integrated Defendant's Azure and/or Azure Cognitive Services platforms.

22. Defendant Microsoft Corporation is a Washington corporation with its headquarters in Redmond, Washington. Defendant maintains a registered agent in Illinois, is licensed to conduct business in Illinois, and does, in fact, conduct substantial business (including business stemming from and/or related to its Azure and ACS platforms) throughout Illinois, including in Cook County.

JURISDICTION AND VENUE

23. This Court has personal jurisdiction over Defendant because (1) during the relevant time period, Defendant was registered to and did, in fact, conduct business in Illinois,

(2) the biometrics that give rise to this lawsuit belong to Illinois residents, (3) the biometrics that give rise to this lawsuit were collected, by Defendant, from individuals located in Illinois, and (4) the BPSAA are used, and interface with and/or integrate Azure and/or ACS, in this State.

24. Venue is proper in this County pursuant to 735 ILCS 5/2-102(a) because Defendant conducts their usual and customary business in this County. 735 ILCS 5/2-102(a).

FACTUAL BACKGROUND

I. Illinois's Biometric Information Privacy Act

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

> (l) 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 or the subject's legally authorized representative."

740 ILCS 14/15 (b).

26. Section 15(a) of BIPA also provides:

> 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.

740 ILCS 14/15(a).

27. As alleged below, Defendant's practices of collecting, storing, and/or using individuals' biometric identifiers and biometric information without obtaining informed written consent violate all three prongs of § 15(b) of BIPA. Additionally, Defendant's failure to provide a publicly available written policy regarding a schedule and guidelines for the retention and permanent destruction of individuals' biometric identifiers and biometric information violates § 15(a) of BIPA.

II. Defendant Violates Illinois's Biometric Information Privacy Act

28. Microsoft Azure ("Azure") is "a public cloud"[3] platform owned and operated by Defendant Microsoft that makes computing resources and services (such as "servers and storage"[4]) available, over the public Internet, to "anyone who wants to use or purchase them."[5] Although cloud computing services, like Azure, "are barely a decade old, [] a variety of organizations—from tiny startups to global corporations, government agencies to non-profits—are embracing the technology for all sorts of reasons."[6] Through Azure and its analogs, it is possible to, *inter alia*, "[q]uickly build, deploy, and scale applications"; "[s]tore, back up, and recover data"; "[s]tream audio and video"; "[d]eliver software on demand"; "[t]est and build

[3] https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-computing/#cloud-deployment-types.

[4] *Id.*

[5] https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-public-cloud/.

[6] *Id.*

applications"; and "[a]nalyze data" with "cloud services, such as machine learning and artificial intelligence, to uncover insights[.]"[7] For Azure customers, these benefits are coupled with the fact that "public clouds can save companies from the expensive costs of having to purchase, manage, and maintain on-premises hardware and application infrastructure – the cloud service provider [(i.e., Microsoft)] is held responsible for all management and maintenance of the system."[8]

29. One of the "more than 200 products and cloud services"[9] comprised by Azure is Azure Cognitive Services ("ACS"), which "are cloud-based artificial intelligence (AI) services that help developers build cognitive intelligence into applications without having direct AI or data science skills or knowledge[]"[10] and "enable[] developers to easily add cognitive features into their applications with cognitive solutions that can see, hear, speak, and analyze."[11]

30. Using ACS's Vision APIs, Microsoft's clients may deploy "Computer Vision" (which "provides you with access to advanced cognitive algorithms for processing images and returning information[]"[12]), "Custom Vision" (which "lets you build, deploy, and improve your own image classifiers. An image classifier is an AI service that applies labels to images, based

[7] *Id.*

[8] https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-public-cloud/.

[9] https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-azure/.

[10] https://learn.microsoft.com/en-us/azure/cognitive-services/what-are-cognitive-services.

[11] *Id.*

[12] *Id.*

on their visual characteristics[]"[13]), and "Face" (which "provides access to advanced face algorithms, enabling face attribute detection and recognition[]"[14]) services.

31. With ACS's Speech APIs, Microsoft's clients may deploy "Speech [S]ervice" which "adds speech-enabled features to applications."[15] Speech Service includes various capabilities, including speech-to-text (allowing users to "[t]ranscribe audible speech into readable, searchable text[]"[16]), text-to-speech (allowing users to "[c]onvert text to lifelike speech for more natural interfaces[]"[17]), speech translation (allowing users to "[i]ntegrate real-time speech translation into [] apps[]"[18]), and speaker recognition (allowing users to "[i]dentify and verify the people speaking based on audio[]"[19]).

32. Through ACS's Language APIs, Microsoft's clients may deploy "Language" (which "provides several Natural Language Processing (NLP) features to understand and analyze text."[20] Natural Language Processing is "the branch of computer science—and more specifically, the branch of artificial intelligence or AI—concerned with giving computers the ability to understand text and spoken words in much the same way human beings can."[21]),

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] https://azure.microsoft.com/en-us/products/cognitive-services/#api.

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] https://learn.microsoft.com/en-us/azure/cognitive-services/what-are-cognitive-services.

[21] https://www.ibm.com/cloud/learn/natural-language-processing.

"Translator" (which "provides machine-based text translation in near real time. Services[]"[22]), "Language Understanding LUIS" ("a cloud-based conversational AI service that applies custom machine-learning intelligence to a user's conversational or natural language text to predict overall meaning and pull out relevant information[]"[23]), and "QnA Maker" (which "allows you to build a question and answer service from your semi-structured content[]"[24]) services.

33. Microsoft sells access to its Azure and/or ACS platforms to clients ("Biometrics Products and/or Services that interface with and/or integrate Azure and/or ACS" or "BPSAA") that (1) collect, capture, and/or otherwise obtain; (2) store; and/or (3) make use of individuals' ("BPSAA subjects") biometric identifiers and biometric information.

34. One such Microsoft client is Brainshark, a purveyor of "sales enablement and readiness solutions[.]"[25] Brainshark has been a Microsoft customer[26] and "close partner"[27] since the company's beginnings, in 1999,[28] and Brainshark has been featured prominently in public-facing case studies published on Microsoft's website as recently as 2017.[29][30] Per Michael Ferioli, VP of Engineering for Brainshark, the very "'first lines of code for [Brainshark's] solution were

[22] https://learn.microsoft.com/en-us/azure/cognitive-services/what-are-cognitive-services.

[23] *Id.*

[24] *Id.*

[25] https://www.prnewswire.com/news-releases/brainsharks-new-ai-powered-engine-elevates-sales-coaching-and-readiness-300659319.html.

[26] https://www.brainshark.com/sites/default/files/microsoft-case-study-brainshark.pdf.

[27] *Id.*

[28] *Id.*

[29] https://partner.microsoft.com/en-us/case-studies/brainshark.

[30] https://www.brainshark.com/sites/default/files/microsoft-case-study-brainshark.pdf.

written using Microsoft technologies—developing in C and using .NET with SQL Server in the back end[.]'"[31] Today, "[u]sing a full suite of Microsoft technologies, the new Brainshark sales training solution provides a completely immersive simulation environment where sales people can practice and master their presentation performance before ever standing in front of a live client[,]"[32] including through Brainshark's convenience-enhancing "integration with Microsoft Dynamics 365[,]"[33] which is "Microsoft's CRM application."[34]

35. The "full suite" of Microsoft technologies employed by Brainshark includes, for one, Azure; Brainshark's website confirms that "Brainshark is hosted in . . . Azure US-East and US-West[]"[35] servers. "According to Ferioli, 'By moving video to Azure we've virtually eliminated the management and cost of maintenance we used to incur. We actually spend less with Microsoft than we thought we would on an ongoing basis.'"[36] Additionally, in or around April of 2017, Brainshark moved "disaster recovery to the Azure cloud."[37]

36. Brainshark's products are also "driven by the artificial intelligence algorithms (vision, speech, language, knowledge) and machine learning capabilities of Azure Cognitive

[31] *Id.*

[32] *Id.*

[33] https://www.brainshark.com/ideas-blog/drive-better-sales-productivity-with-brainshark-and-microsoft-dynamics-365/.

[34] *Id.*

[35] https://brainshark.zendesk.com/hc/en-us/articles/360044325192-Why-am-I-having-issues-viewing-content-in-Mainland-China-.

[36] https://www.brainshark.com/sites/default/files/microsoft-case-study-brainshark.pdf.

[37] https://www.buurst.com/2017/04/19/brainshark-chooses-softnas/.

Services."[38][39] Given "Microsoft's newest developments in augmented reality, motion sensing, biometrics, artificial intelligence, machine learning, and analytics[,]"[40][41] Brainshark is able to track the "body language, and facial expression[s]"[42] of its users as to assess their levels of "comfort and confidence[.]"[43]

37. That is, Brainshark's video-based sales coaching[44] gives "automated, actionable insights that help ensure salespeople master critical messages before they get in front of a buyer."[45] To receive this coaching (i.e., when practicing their elevator pitch,[46] learning how to market a new product, reviewing how to best handle common objections,[47] or refining their other skills), a sales representative, first, records a video of themself and uploads it to Brainshark's platform.[48]

[38] https://www.brainshark.com/sites/default/files/microsoft-case-study-brainshark.pdf.

[39] https://www.youtube.com/watch?v=uVl5ar7TNx8.

[40] https://www.brainshark.com/sites/default/files/microsoft-case-study-brainshark.pdf.

[41] https://partner.microsoft.com/en-us/case-studies/brainshark.

[42] *Id.*

[43] *Id.*

[44] https://www.prnewswire.com/news-releases/brainsharks-new-ai-powered-engine-elevates-sales-coaching-and-readiness-300659319.html.

[45] *Id.*

[46] https://www.techtarget.com/searchcustomerexperience/feature/Sales-enablement-best-practices-to-enhance-customer-interactions.

[47] https://www.prnewswire.com/news-releases/brainsharks-new-ai-powered-engine-elevates-sales-coaching-and-readiness-300659319.html.

[48] https://www.techtarget.com/searchcustomerexperience/feature/Sales-enablement-best-practices-to-enhance-customer-interactions.

38. Then, Brainshark utilizes Machine Analysis technology[49] to "measure, score and certify" the preparedness of the sales representative[50] and deliver performance feedback.[51] This Machine Analysis "transcribes the videos[,]"[52] "factor[s] in whether sellers adhere to manager-defined parameters, including coverage of key topics, speaking rate, low level of filler words ("um," "uh," etc.)[,]"[53] and provides other personalized insights.

39. Such insights include: (1) "Emotion analysis – Every second of the video, Machine Analysis analyzes the seller's facial expression for eight emotions – happiness, surprise, sadness, contempt, etc. – noting their frequency within a submission (e.g., 95% happiness, 2% sadness, 3% contempt, etc.). Managers and reps can replay the video from within Brainshark's platform, viewing the exact moments when emotion changes are noted" [54]; and (2) "Personality insights – Measuring the frequency of certain categories of words, the engine detects how often the participant displays traits such as openness, conscientiousness, extraversion, agreeableness and an emotional range, to show how sellers could be perceived by buyers."[55]

[49] https://www.prnewswire.com/news-releases/brainsharks-new-ai-powered-engine-elevates-sales-coaching-and-readiness-300659319.html.

[50] https://www.brainshark.com/platform/#tab-3.

[51] https://www.techtarget.com/searchcustomerexperience/feature/Sales-enablement-best-practices-to-enhance-customer-interactions.

[52] https://www.prnewswire.com/news-releases/brainsharks-new-ai-powered-engine-elevates-sales-coaching-and-readiness-300659319.html.

[53] *Id.*

[54] *Id.*

[55] *Id.*

40. In conducting this analysis of individuals' emotions (as evinced by their facial expressions), Brainshark (1) collects, captures, and/or otherwise obtains; (2) stores; and/or (3) makes use of such individuals' biometric identifiers (namely, scans of facial geometry) and biometric information.[56]

41. As Brainshark's software interfaces with and/or integrates Azure and/or ACS, Defendant Microsoft also (1) collects, captures, and/or otherwise obtains; (2) stores; and/or (3) makes use of such individuals' biometric identifiers and biometric information.

42. Microsoft sells access to its Azure and/or ACS platforms to additional clients ("Biometrics Products and/or Services that interface with and/or integrate Azure and/or ACS" or "BPSAA") that (1) collect, capture, and/or otherwise obtain; (2) store; and/or (3) make use of individuals' ("BPSAA subjects") biometric identifiers and biometric information.

43. By way of BPSAA, Defendant (1) collects, captures, and/or otherwise obtains; (2) stores; and/or (3) makes use of the biometric identifiers and biometric information from a multitude of BPSAA subjects.

44. Yet Defendant has failed to comply with the foregoing provisions of § 15(a) and § 15(b) of BIPA.

III. Plaintiff's Experience

45. Plaintiff Cody Clark's biometric identifier (scan of facial geometry) and biometric information were collected, captured, otherwise obtained, and/or stored by Brainshark in or around August 2020, when he was (1) located in Illinois, (2) carrying out his job duties as a

[56] *See* Mem. Op. and Order, ECF No. 45 at PageID #254-258, *Wilk v. Brainshark, Inc.*, No. 1:21-cv-04794 (N.D. Ill. Sept. 27, 2022).

salesperson with CONMED Corporation ("CONMED"),[57] and (3) interacting with Brainshark's video-based coaching technology.

46. Brainshark supplied Mr. Clark with feedback regarding his efforts to refine his professional skills and, in doing so, analyzed his facial expressions. Thus, Brainshark (1) collected, captured, and/or otherwise obtained; (2) stored; and/or (3) made use of Mr. Clark's biometric identifier(s) (namely, scans of his facial geometry) and/or biometric information.

47. As Brainshark's software interfaces with and/or integrates Azure and/or ACS, Defendant Microsoft also (1) collected, captured, and/or otherwise obtained; (2) stored; and/or (3) made use of Mr. Clark's biometric identifier(s) and/or biometric information.

48. Microsoft sells access to its Azure and/or ACS platforms to other clients ("Biometrics Products and/or Services that interface with and/or integrate Azure and/or ACS" or "BPSAA") that (1) collect, capture, and/or otherwise obtain; (2) store; and/or (3) make use of individuals' ("BPSAA subjects") biometric identifiers and biometric information.

49. By way of BPSAA, Defendant (1) collects, captures, and/or otherwise obtains; (2) stores; and/or (3) makes use of the biometric identifiers and biometric information from a multitude of BPSAA subjects.

50. That is to say, Defendant Microsoft's having (1) collected, captured, and/or otherwise obtained; (2) stored; and/or (3) made use of Mr. Clark's biometric identifier(s) and/or biometric information was, lamentably, not anomalous.

51. However, at no time did Plaintiff Cody Clark receive notice from Defendant Microsoft, in writing or any other form, that Defendant Microsoft was collecting, storing, and using his biometrics.

[57] https://www.conmed.com/en-us/.

52. At no time did Plaintiff Cody Clark receive notice from Defendant Microsoft, in writing or any other form, of the specific purpose and length of term for which his biometrics were being collected, stored, and used by Defendant Microsoft.

53. At no time was Plaintiff Cody Clark asked, by Defendant Microsoft, to provide consent for Defendant Microsoft to collect, store, or use his biometrics.

54. At no time did Plaintiff Cody Clark give Defendant Microsoft permission in writing or any other form for – or otherwise consent or agree to – the collection, storage, or use of his biometrics.

55. Likewise, Defendant Microsoft never provided Plaintiff Cody Clark with any opportunity to prohibit or prevent the collection, storage, or use of his biometrics.

56. Upon information and belief, at no time, while possessing Plaintiff Cody Clark's biometric data, did Defendant Microsoft maintain publicly available retention and deletion schedules for biometric data.

57. By collecting Plaintiff Cody Clark's unique biometrics without his consent, written or otherwise, Defendant Microsoft invaded Plaintiff Cody Clark's statutorily protected right to privacy in his biometrics.

CLASS ALLEGATIONS

58. **Class Definition**: Plaintiff Cody Clark brings this action pursuant to 735 ILCS 5/2-801 on behalf of a class of similarly situated individuals, defined as follows (the "Class"):

> All Illinois residents whose biometric identifiers and/or biometric information were collected, captured, otherwise obtained, stored, used, transmitted, or disseminated by Microsoft, by way of products and/or services that interfaced with and/or integrated Azure and/or Azure Cognitive Services.

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

60. **Numerosity:** Pursuant to 735 ILCS 5/2-801 (1), the numbers of persons within the Class and Subclasses are substantial, each believed to amount to thousands if not millions of persons. It is, therefore, impractical to join each member of the Class as a named Plaintiff. Further, the size and relatively modest value of the claims of the individual members of the Class renders joinder impractical. Accordingly, utilization of the class action mechanism is the most economically feasible means of determining and adjudicating the merits of this litigation. Moreover, the Classes are ascertainable and identifiable from Defendants' records.

61. **Commonality and Predominance:** Pursuant to 735 ILCS 5/2-801(2), there are well-defined common questions of fact and law that exist as to all members of the Classes and that predominate over any questions affecting only individual members of the Classes. 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 collected or otherwise obtained Plaintiff's and the Class's biometric identifiers and/or biometric information;

(b) whether Defendant properly informed Plaintiff and the Class that they collected, used, and stored their biometric identifiers and/or biometric information;

(c) whether Defendant obtained written release (as defined in 740 ILCS 1410) to collect, use, and store Plaintiff's and the Class's biometric identifiers and/or biometric information;

(d) whether Defendant developed 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 their last interaction, whichever occurs first;

(e) whether Defendant used Plaintiff's and the Class's biometric identifiers and/or biometric information to identify them;

(f) whether Defendant destroyed Plaintiff's and the Class's biometric identifiers and/or biometric information once that information was no longer needed for the purpose for which it was originally collected; and

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

62. **Adequate Representation:** Pursuant to 735 ILCS 5/2-801 (3), Plaintiff has retained and is represented by qualified and competent counsel who are highly experienced in complex consumer class action litigation. Plaintiff and his counsel are committed to vigorously prosecuting this class action. Moreover, Plaintiff is able to fairly and adequately represent and protect the interests of the Class. Neither Plaintiff nor his counsel have any interest adverse to, or in conflict with, the interests of the absent members of the Class. Plaintiff has raised viable statutory claims or the type reasonably expected to be raised by members of the Class, and will vigorously pursue those claims. If necessary, Plaintiff may seek leave of this Court to amend this Class Action Complaint to include additional Class representatives to represent the Class, add additional claims as may be appropriate, or amend the Class definition to address any steps that Defendant took.

63. **Superiority:** Pursuant to 735 ILCS 5/2-801(4), 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 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 issues. By contrast, the maintenance of this action as a class action, with respect to some or all of the issues presented herein, 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. Plaintiff anticipates no difficulty in the management of this action as a class action. Class-wide relief is essential to compliance with BIPA.

COUNT I – FOR DAMAGES AGAINST DEFENDANT
Violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.*
(On behalf of Plaintiff and the Class)

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

65. Defendant Microsoft is a corporation and qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

66. BIPA requires that private entities, such as Defendant, obtain informed written consent from individuals before acquiring their biometrics. Specifically, BIPA makes it unlawful to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or customer's biometric identifiers or biometric information unless [the entity] first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or

stored; (2) informs the subject . . . in writing of the specific purpose and length of for which a biometric identifier or biometric information is being captured, collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information . . . ." 740 ILCS 14/15(b).

67. BIPA also requires that a private entity in possession of biometric identifiers and/or biometric information establish and maintain a publicly available retention policy. An entity which possesses biometric identifiers or information must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric information (entities may not retain biometric information longer than three years after the last interaction with the individual); and (ii) adhere to the publicly posted retention and deletion schedule.

68. Microsoft sells access to its Azure and/or ACS platforms to clients ("Biometrics Products and/or Services that interface with and/or integrate Azure and/or ACS" or "BPSAA")[58] that (1) collect, capture, and/or otherwise obtain; (2) store; and/or (3) make use of individuals' ("BPSAA subjects") biometric identifiers and biometric information.

69. Plaintiff and the other Class members are BPSAA subjects; they have interacted with BPSAA.

[58] One such BPSAA is a video-based coaching tool that was purveyed by Brainshark and utilized by Plaintiff Clark. This tool (1) collected, captured, and/or otherwise obtained; (2) stored; and/or (3) made use of Plaintiff Clark's and other individuals' biometric identifiers (namely, scans of facial geometry) and/or biometric information as to conduct assessments of Mr. Clark's and other users' facial expressions. These facial expression assessments informed automated feedback that Brainshark conferred to Mr. Clark and other users, which included "emotion analysis" and "personality insights."

70. By way of BPSAA, Defendant (1) collects, captures, and/or otherwise obtains; (2) stores; and/or (3) makes use of the biometric identifiers and biometric information from a multitude of BPSAA subjects.

71. Microsoft did so without valid consent, without complying with, and, thus, in violation of BIPA.

72. Defendant's practices with respect to capturing, collecting, storing, and using Plaintiff's and the Class members' biometrics fail to comply with applicable BIPA requirements:

a. Defendant failed to inform Plaintiff and the other members of the Classes in writing that their biometrics were being collected and stored, prior to such collection or storage, as required by 740 ILCS 14/15(b)(1);

b. Defendant failed to inform Plaintiff and the other Class members in writing of the specific purpose for which their biometrics were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(2);

c. Defendant failed to inform Plaintiff and the other Class members in writing of the specific length of term for which their biometrics were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(2);

d. Defendant failed to obtain a written release, as required by 740 ILCS 14/15(b)(3);

e. Defendant failed to provide a publicly available retention schedule detailing the length of time for which the biometrics are stored and/or guidelines for permanently destroying the biometrics they store, as required by 740 ILCS 14/15(a); and,

f. Defendant failed to obtain informed consent to disclose or disseminate the Class members' biometrics for purposes of data retention and storage of the same, as required by 740 ILCS 14/15(d)(1).

73. By using the biometrics mentioned *supra* to further refine its technologies and/or provide services to its clients, Defendant Microsoft profited from Plaintiff's and the other Class members' biometrics, in violation of 740 ILCS 14/15(c).

74. Defendant knew, or was reckless in not knowing, that its Azure and Azure Cognitive Services technologies would be subject to the provisions of BIPA, yet Defendant failed to comply with the statute.

75. By capturing, collecting, storing, using, and/or disseminating Plaintiff's and the other Class members' biometrics as described herein, Defendant denied Plaintiff and the other Class members their rights to statutorily required information and violated their respective rights to biometric information privacy, as set forth in BIPA.

76. BIPA provides for statutory damages of $5,000 for each willful and/or reckless violation of BIPA and, alternatively, damages of $1,000 for each negligent violation of BIPA. 740 ILCS 14/20(1)–(2).

77. Defendant's violations of BIPA, a statute that has been in effect in all relevant times, were knowing and willful, or were at least in reckless disregard of the statutory requirements. Alternatively, Defendant negligently failed to comply with BIPA.

78. Accordingly, with respect to Count I, Plaintiff, individually and on behalf of the proposed Class, prays for the relief set forth below.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Cody Clark, on behalf of himself 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 Plaintiff as representative 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 pursuant to 740 ILCS 14/20(2), or, alternatively, statutory damages of $1,000.00 for each and every violation pursuant to 740 ILCS 14/20(1) if Defendant's violations are found to have been committed negligently;

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 collect, store, and use biometric identifiers or biometric information in compliance with BIPA;

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

F. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and

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

JURY TRIAL

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

Dated: December 23, 2022

Respectfully submitted,

/s/ Carl V. Malmstrom .
WOLF HALDENSTEIN ADLER
FREEMAN & HERZ LLC
Carl V. Malmstrom
Attorney No. 38819
111 W. Jackson Blvd., Suite 1700
Chicago, IL 60604
Tel: (312) 984-0000
Fax: (212) 686-0114
E-mail: malmstrom@whafh.com

Local Counsel for Plaintiff and the

Putative Class

BURSOR & FISHER, P.A.
Philip L. Fraietta
Attorney No. 6337165
Joseph I. Marchese*
888 Seventh Avenue
New York, NY 10019
Tel: (646) 837-7150
Fax: (212) 989-9163
jmarchese@bursor.com
pfraietta@bursor.com

**Pro Hac Vice Application Forthcoming*

Counsel for Plaintiff and the
Putative Class