1
2
3
4
5
6
7

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

CAROL COOPER, individually and on behalf of all others similarly situated,	NO.
Plaintiff,	**CLASS ACTION COMPLAINT**
v.	JURY DEMANDED
AMAZON.COM, INC., a Delaware corporation, and AMAZON.COM SERVICES, LLC, a Delaware limited liability company,	
Defendants.	

<u>CLASS ACTION COMPLAINT</u>

Plaintiff, Carol Cooper, on behalf of herself and all others similarly situated, for her

Class Action Complaint against Defendants Amazon.com, Inc., and Amazon.com Services,

LLC (collectively, "Amazon"), states as follows:

<u>PARTIES</u>

1. Plaintiff is an Illinois citizen residing in Madison County, Illinois.

2. Defendant Amazon.com, Inc. is a Delaware corporation with its principal place

of business located in Washington.

CLASS ACTION COMPLAINT - 1

3.   Defendant Amazon.com Services, LLC is a Delaware limited liability company with its principal place of business located in Washington.[1]

JURISDICTION AND VENUE

4.   This Court has jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d). Because Plaintiff and Defendants are citizens of different states, there is minimal diversity. The total claims of Class Members exceed $5,000,000 exclusive of interest and costs. There are at least 100 Class Members.

5.   This Court has personal jurisdiction over Defendants because they have their principal place of business in Washington and are, therefore, citizens of Washington.

6.   Venue is proper in this district pursuant to 28 U.S.C. § 1391 because Defendants reside in this district and are residents of the State in which the district is located.

NATURE OF THE ACTION

7.   This claim involves Illinois' Biometric Information Privacy Act, 740 ILCS 14/1 *et seq*. ("BIPA"), a law that regulates companies that collect, store, and use Illinois citizens' biometric data, such as fingerprints, scans of face geometry, and voiceprints, and information derived therefrom.

8.   Amazon is the world's leading e-commerce platform, with net sales of $280 billion in 2019. Of that $280 billion, $193 billion was from the United States alone.[2]

9.   According to James Marcus, an early employee of Amazon who became senior editor of Amazon.com: "It was made clear from the beginning that data collection was also one

---

[1] Defendants Amazon.com Inc. and Amazon.com Services LLC are collectively referred to herein as "Amazon."

[2] Form 10-K, Amazon.com, Inc., *available at* https://www.sec.gov/ix?doc=/Archives/edgar/data/1018724/000101872420000004/amzn-

CLASS ACTION COMPLAINT - 2

of Amazon's businesses. All customer behavior that flowed through the site was recorded and

tracked. And that itself was a valuable commodity."[3]

  10. Amazon provides many services using its "Alexa" voice-based virtual assistant.

  11. Alexa is embedded in many devices, ranging from Amazon's own Echo "smart"

speakers and Fire tablets, to many other "smart" items made by other companies. Currently,

Alexa is integrated into and compatible with over 100,000 products, such as phones, TVs,

thermostats, ovens, lights, locks, rings, light bulbs, headphones, and automobiles.[4]

  12. After a user speaks to an Alexa device, Amazon collects, captures, or otherwise

obtains, and subsequently stores voiceprints of the user, and transcriptions of the voiceprints.

  13. These voiceprints and transcriptions constitute "biometric identifiers" and/or

"biometric information" regulated by BIPA, and over the past five years, Amazon has violated

Plaintiff and the Class Members rights under BIPA, on numerous occasions, by, *inter alia*:

- systematically and intentionally collecting, obtaining, using and/or storing biometric identifiers and/or biometric information without first obtaining the written release executed by Plaintiff and Class Members required by 740 ILCS 14/15(b)(3);

- not properly informing Plaintiff and Class Members in writing that their biometric identifiers and/or biometric information was being collected and/or stored as required by 740 ILCS 14/15(b)(1);

- not informing Plaintiff and Class Members in writing of the specific purpose and length of term for which her biometric

---

20191231x10k.htm#s0EE73FEFBB6A5BD49E6C88DF6043F8A5.

[3] PBS Frontline, *Amazon Empire: The Rise and Reign of Jeff Bezos* (hereafter "PBS Frontline"), transcript available at https://www.pbs.org/wgbh/frontline/film/amazon-empire/transcript/ (last visited June 24, 2021) [hereinafter PBS Frontline].

[4] Cinnamon Janzer, et al., *Everything that Works with Amazon Echo and Alexa* (Updated May 8, 2019), https://www.reviewed.com/smarthome/features/everything-that-works-with-amazon-echo-alexa; *see also* PBS Frontline.

CLASS ACTION COMPLAINT - 3

identifiers and/or biometric information was being collected, stored, and used as required by 740 ILCS 14/15(b)(2);

- not developing and making available a written policy establishing a retention schedule and guidelines for permanently destroying biometric identifiers and/or biometric information as required by 740 ILCS 14/15(a);

- selling, leasing, trading, or otherwise profiting from Plaintiff's and Class Members' biometric identifiers and/or biometric information in violation of 740 ILCS 14/15(c);

- disclosing, redisclosing, or otherwise disseminating Plaintiff's and Class Members' biometric identifiers and/or biometric information to third parties, without satisfying the requirements of 740 ILCS 14/15(d)(1)-(4);

- not storing, transmitting, and/or protecting from disclosure Plaintiff's and Class Members' biometric identifiers and/or biometric information using the reasonable standard of care within the industry, in violation of 740 ILCS 14/15(e)(1); and/or

- not storing, transmitting, and/or protecting from disclosure Plaintiff's and Class Members' biometric identifiers and/or biometric information in a manner that is the same as or more protective than the manner in which Amazon stores, transmits, and protects other confidential and sensitive information, in violation of 740 ILCS 14/15(e)(2).

14.   Accordingly, Plaintiff seeks to represent a class of similarly situated individuals to obtain an Order: (A) awarding Plaintiff and each Class Member statutory damages of $5,000 for each willful and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14.20(1); (B) enjoining Amazon from collecting, obtaining, storing, using, selling, leasing, trading, profiting from, disclosing, redisclosing, or otherwise disseminating Plaintiff's and the Class Members' biometric identifiers and biometric information until done so in compliance with BIPA; (C) awarding Plaintiff and the Class Members reasonable attorneys'

CLASS ACTION COMPLAINT - 4

fees, costs, and other expenses pursuant to 740 ILCS 14/20(3); (D) awarding Plaintiff and the

Class Members pre-and post-judgment interest, as provided by law; and (E) awarding such

other and further relief as is just and appropriate.

Illinois' Biometric Information Privacy Act

15.   The Illinois General Assembly enacted the Biometric Information Privacy Act,

740 ILCS 14/*et seq*. ("BIPA") in 2008 to establish standards of conduct for private entities that

collect or possess biometric identifiers and biometric information.

16.   The Illinois General Assembly noted that BIPA was carefully crafted to protect

biometric data because "unlike other unique identifiers that are used to access finances or other

sensitive information," one's own biometric information cannot be changed; "[t]herefore, 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.

17.   "Biometric identifiers" covered by BIPA include retina or iris scans,

fingerprints, voiceprints, and scans of human or face geometry, none of which can be changed

if compromised. 740 ILCS 14/10.

18.   "Biometric information" covered by BIPA includes "any information, regardless

of how it is captured, converted, stored, or shared, based on an individual's biometric identifier

used to identify an individual." *Id.*

19.   BIPA makes it unlawful for any private entity to, *inter alia*, "collect, capture,

purchase, receive through trade, or otherwise obtain a person's or a customer's biometric

identifier or biometric information unless it first: (1) informs the subject . . . in writing that a

biometric identifier or biometric information is being collected or stored; (2) informs the

subject . . . in writing of the specific purpose and length of term for which a biometric identifier

CLASS ACTION COMPLAINT - 5

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 . . . ." 740 ILCS 14/15(b).

20.   Furthermore, BIPA requires that any "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).

21.   BIPA also provides that "[n]o private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information." 740 ILCS 14/15(c).

22.   BIPA further makes it unlawful for any private entity in possession of a biometric identifier to "disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless: (1) the subject of the biometric identifier or biometric information . . . consents to the disclosure or redisclosure; (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier . . . ; (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or (4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction." 740 ILCS 14/15(d).

23.   Finally, BIPA provides that "[a] private entity in possession of a biometric identifier or biometric information shall: (1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the

CLASS ACTION COMPLAINT - 6

private entity's industry; and (2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

24.   BIPA provides for a private right of action: "Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party." 740 ILCS 14/20.

25.   The Illinois Supreme Court has explained that a person whose biometric identifiers are the subject of violations of section 15 of BIPA is "aggrieved" by the entity's failure to comply with BIPA and is "entitled to seek recovery" under Section 14/20. *Rosenbach v. Six Flags Entm't Corp*, 2019 IL 123186, ¶ 33 ("[W]hen a private entity fails to comply with one of section 15's requirements, that violation constitutes an invasion, impairment, or denial of the statutory rights of any person or customer whose biometric identifier or biometric information is subject to the breach. Consistent with the authority cited above, such a person or customer would clearly be 'aggrieved' within the meaning of section 20 of the Act (*id.* § 20) and entitled to seek recovery under that provision. No additional consequences need be pleaded or proved. The violation, in itself, is sufficient to support the individual's or customer's statutory cause of action.").

26.   Under BIPA, "[a] prevailing party may recover *for each violation*: (1) against a private entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater; (2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater; (3) reasonable attorneys' fees and costs, including expert witness fees and other

CLASS ACTION COMPLAINT - 7

1   litigation expenses; and (4) other relief, including an injunction, as the State or federal court

2   may deem appropriate." *Id.* (emphasis added).

3   27.   Under BIPA, each instance of collecting and/or disclosing a person's biometric

4   data without consent constitutes a separate violation for which recovery can be had. *See*

5   *Cothron v. White Castle Sys., Inc.*, 477 F. Supp. 3d 723, 732–34 (N.D. Ill. 2020) ("[The

6   statutory] text is unambiguous and therefore dispositive. A party violates Section 15(b) when it

7   collects, captures, or otherwise obtains a person's biometric information without prior informed

8   consent. This is true the first time an entity scans a fingerprint or otherwise collects biometric

9   information, but it is no less true with each subsequent scan or collection. . . . The language of

10   Section 15(d) requires the same result. . . . [T]he Court is bound by the clear text of the

11   statute . . . . [I]t is not the role of a court—particularly a federal court—to rewrite a state statute

12   to avoid a construction that may penalize violations severely. . . . In sum, the Court concludes

13   that [the plaintiff] has alleged multiple timely violations of both Section 15(b) and Section

14   15(d). According to BIPA Section 20, she can recover 'for each violation.' 740 ILCS 14/20.").

15   **How Alexa Works**

16   28.   Alexa devices are designed to record and respond to oral communications upon

17   hearing a "wake word" (usually "Alexa").

18   29.   If the "wake word" is not spoken, Amazon claims that Alexa-enabled devices

19   will not capture a user's conversations.[5]

---

[5] *Alexa and Alexa Device FAQ's*, Amazon.com, https://www.amazon.com/gp/help/customer/
display.html?linkCode=w61&imprToken=28-fLyu75f7XPVZKlgVB7w&slotNum=0&nodeId=
201602230 (last visited July 8, 2021).

CLASS ACTION COMPLAINT - 8

30.   Despite Amazon's claim that Alexa only captures conversations after hearing the "wake word," reports and studies have indicated that Alexa-enabled devices frequently capture conversations by accident without being triggered by the "wake word."[6]

31.   One group of researchers discovered more than 1,000 sequences of words that incorrectly trigger smart speakers, such as Alexa. For example, Alexa may inadvertently be activated by the words "unacceptable" or "election."[7]

32.   Amazon's "wake word" technology works by identifying acoustic patterns that match the wake word.

33.   Once the Alexa device recognizes the acoustical pattern of the wake work, the device captures a voiceprint of the speaker's oral communication that follows the wake word and transmits the voiceprint to Amazon to undergo a series of steps to process a response using Amazon's Alexa Voice Service.

34.   The Alexa Voice Service utilizes Automatic Speech Recognition technology (ASR), whereby computers detect patterns in audio waveforms of the voiceprint, match them with the sounds in a given language, and ultimately identify the words spoken.[8] This is the first step required for Alexa to respond to a request.

---

[6] *See, e.g.*, Tom Warren, *Amazon explains how Alexa recorded a private conversation and sent it to another user* (May 24, 2018), https://www.theverge.com/2018/5/24/17391898/amazon-alexa-private-conversation-recording-explanation; Sara Morrison, *Alexa records you more often than you think* (Feb. 21, 2020), https://www.vox.com/recode/2020/2/21/21032140/alexa-amazon-google-home-siri-apple-microsoft-cortana-recording; Matt Day, et al., *Is Anyone Listening to You on Alexa? A Global Team Reviews* (Apr. 10, 2019), https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio.

[7] *See* Lea Schönherr, et al., *"Unacceptable, where is my privacy?" Exploring Accidental Triggers of Smart Speakers*, https://unacceptable-privacy.github.io/ (last visited July 8, 2021); *see also* Lea Schönherr, et al., *"Unacceptable, where is my privacy?" Exploring Accidental Triggers of Smart Speakers* (Aug. 2, 2020), https://arxiv.org/pdf/2008.00508.pdf.

[8] *What Is Automatic Speech Recognition?*, Amazon.com, https://developer.amazon.com/en-US/alexa/alexa-skills-kit/asr (last visited Feb. 19, 2020).

CLASS ACTION COMPLAINT - 9

35.   The ASR technology analyzes various features of the user's voiceprint, such as the micro pauses the speaker takes between words, the frequency, and the speaker's pitch, in order to convert the voiceprint into a transcribed text string.[9]

36.   After the ASR analyzes and transcribes the voiceprint, the Alexa Voice Service interprets the text using Natural Language Understanding (NLU), a process that allows Alexa to deduce what a speaker intends, rather than just the words they say.[10]

37.   According to Amazon, NLU works by using prior users' input: "With NLU, Alexa devices like Amazon Echo can apply learnings from historical interactions, across thousands of diverse applications, to understand that 'is it raining outside' and 'is it going to rain' are essentially the same question."[11]

38.   After the NLU has determined what the user wants, the Alexa Voice Service compares the transcribed communication to expected commands and, if it finds a match, it follows a set of instructions to retrieve the appropriate information from a designated data source to provide a response to the user in the form of a simple speech markup language (SSML) which informs Alexa how to respond.

39.   If the NLU does not find a match, it looks for an alternative of what to do based on what information it has.

---

[9] *See* Joseph Frankel, *How Does My Voice Assistant Know What I'm Saying?* (Apr. 20, 2018), https://nymag.com/intelligencer/smarthome/make-me-smarter-voice-speech-recognition-alexa-siri-cortana-google.html; Josh Hendrickson, *Alexa, Siri, and Google Don't Understand a Word You Say* (Feb. 19, 2019) https://www.howtogeek.com/405011/voice-assistants-dont-really-understand-you/; Alexandre Gonfalonieri, *How Amazon Alexa works? Your guide to Natural Language Processing (AI)* (Nov. 21, 2018), https://towardsdatascience.com/how-amazon-alexa-works-your-guide-to-natural-language-processing-ai-7506004709d3.
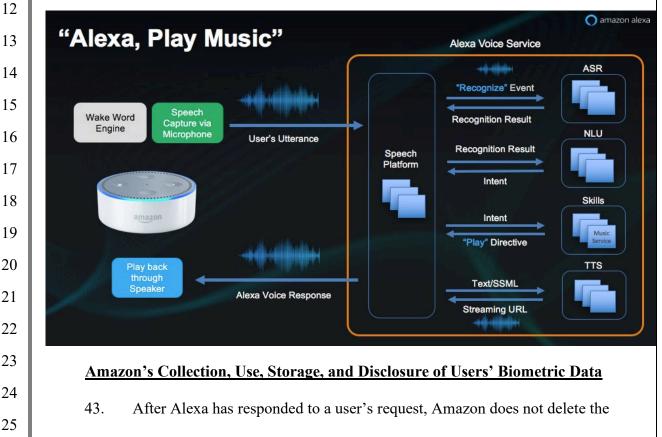
[10] *What Is Natural Language Understanding (NLU)?*, Amazon.com, https://developer.amazon.com/en-US/alexa/alexa-skills-kit/nlu (last visited July 8, 2021).

[11] *Id.*

CLASS ACTION COMPLAINT - 10

40.   Alexa's response system then takes the SSML that was produced, uses a text-to-speech (TTS) system to generate an audio speech file, and streams the audio to the user's device.

41.   Generally, Alexa's response ends the interaction, though in some circumstances, Alexa may ask follow-up questions to the user that require answers in order for Alexa to provide a complete response to the user's inquiry. If a follow-up answer is provided, the Alexa device captures the speaker's voiceprint and the Alexa Voice Service repeats the steps described above.

42.   The speech capture, Alexa Voice Service, and response process is represented below:

Amazon's Collection, Use, Storage, and Disclosure of Users' Biometric Data

43.   After Alexa has responded to a user's request, Amazon does not delete the voiceprint or the transcription created by that request.

CLASS ACTION COMPLAINT - 11

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

44.   Instead, Amazon captures, collects, and indefinitely retains the voiceprint on its servers for continued use and analysis, in order to, *inter alia*, improve its speech and voice recognition capabilities.

45.   For years, Amazon represented that the voiceprints were simply streamed to the cloud and used only to allow Alexa to respond to the command and help personalize Alexa's response to a user.

46.   Amazon has more recently, however, indicated that it stores voiceprints and the transcriptions made from the voiceprints on multiple servers.

47.   Moreover, Amazon captures, collects, and indefinitely retains the voiceprints of users when Alexa activates by mistakenly "hearing" the wake word.

48.   All voiceprints from the Amazon customer are associated with the customer's Amazon account.

49.   Amazon collects, obtains, and stores the voiceprint and transcription created therefrom to improve Alexa via a process known as "machine learning."

50.   Machine learning only works when the artificial intelligence system underlying it is supported with data, from which the system can learn and develop.

51.   In Amazon's case, Alexa's machine learning is bolstered by what likely amounts to hundreds of millions, if not billions, of voiceprints that Amazon has stored on its servers, which it uses to constantly refine the natural language understanding that is critical to Alexa's function.

52.   In addition, according to an article by Bloomberg, Amazon.com, Inc. employs thousands of people around the world, both full-time Amazon employees and third-party

CLASS ACTION COMPLAINT - 12

contractors, who listen to voice recordings, have access to voiceprints, and review the transcriptions captured by Amazon's Echo device.[12]

53.   These Amazon workers transcribe and annotate the aforementioned data as part of an effort to eliminate gaps in Alexa's understanding of human speech and to help it better respond to commands.[13]

54.   The teams also use internal chat rooms to share audio files "when they need help parsing a muddled word—or come across an amusing recording."[14]

55.   Because of Amazon's collection of voiceprints and transcripts thereof, Amazon has been able to significantly improve all of its voice-based products and services to the point that, in August 2019, Amazon reported that Alexa answered queries accurately 80% of the time, up 19 percentage points from 61% in July 2018.[15]

56.   Once Amazon is in possession of the voiceprint, Amazon employees may access it, and identify the location of the device where it was obtained and other data collected by the Alexa device.

57.   Upon information and belief, the voiceprint is also aggregated with data from other Amazon sources, such as the user's shopping history, order history, or reminders to create profiles of information for Amazon to utilize for its own business purposes.

///

---

[12] Matt Day, et al., *Is Anyone Listening to You on Alexa? A Global Team Reviews* (Apr. 10, 2019), https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio.

[13] *Id.*

[14] *Id.*

[15] Rayna Hollander, *Amazon is improving the accuracy of Alexa's natural language understanding* (Oct. 11, 2019), https://www.businessinsider.com/amazon-bolsters-alexa-skill-voice-accuracy-2019-10.

CLASS ACTION COMPLAINT - 13

1
2
3

58.   Amazon does not delete the voiceprints after they have been used to provide a response. Instead, Amazon stores the voiceprints, which Amazon's artificial intelligence and human employees then review for Amazon's business purposes.

4
5
6
7

59.   Amazon does not allow a user to stop it from collecting voiceprints. The only way to stop Amazon's collection of voiceprints is to mute the microphone or deactivate the device, both of which defeat the device's utility.

8
9
10
11

60.   In 2019, Amazon began providing users the ability to delete voice recordings; however, while Amazon's current policies tell customers that they may delete voice recordings, Amazon is unclear as to whether this deletes all of the voiceprints Amazon has collected and the transcriptions made from those voiceprints.[16]

12
13
14
15
16
17
18

61.   For instance, Amazon states that even if a customer deletes an audio recording, Amazon, or third-party developers may retain "records of the interaction. For example, for many types of Alexa requests—such as when a customer subscribes to Amazon Music Unlimited, places an Amazon Fresh order, requests a car from Uber or Lyft, orders a pizza from Dominos, or makes an in-skill purchase of premium digital content—Amazon and/or the applicable skill developer obviously need to keep a record of the transaction."[17]

19
20
21
22

62.   Moreover, as stated by Theresa Payton, a former White House chief information officer and founder of cybersecurity company Fortalice: "'Delete' is never really 'delete.'" "Delete just means that you can't see it anymore."[18]

23
24

[16] *See* Letter from Amazon to Senator Christopher A. Coons; https://www.coons.senate.gov/imo/media/doc/Amazon%20Senator%20Coons__Response%20Letter__6.28.19[3].pdf.

25

[17] *Id.*

26

[18] Alfred Ng, *Amazon Alexa transcripts live on, even after you delete voice records* (May 9, 2019), https://www.cnet.com/home/smart-home/amazon-alexa-transcripts-live-on-even-after-you-delete-voice-records/.

CLASS ACTION COMPLAINT - 14

63.   Amazon does not, and/or within the Class Period failed to, disclose the following to its users:

      A.   that Amazon creates, analyzes, and utilizes a user's voiceprint and that the same is stored on Amazon's servers indefinitely;

      B.   that Amazon creates, analyzes, stores, and utilizes a transcription of a user's request, derived from the aforementioned voiceprint, and stores the same on Amazon's servers indefinitely;

      C.   that human employees and third-party contractors have access to and utilize users' voiceprints and the transcriptions created therefrom, or the extent of such access and use;

      D.   the retention schedule associated with a user's voiceprint and the transcription created from the voiceprint; and

      E.   guidelines for a user to permanently delete all of their voiceprints and the transcriptions made therefrom, from all of Amazon's servers.

64.   Furthermore, Amazon collects, captures, stores, and utilizes the voiceprints and transcriptions derived therefrom without receiving executed written releases from any of the users of Alexa-enabled products.

65.   David Limp, the Senior Vice President of Devices and Services at Amazon.com acknowledged Amazon's inadequate disclosures, and Robert Frederick, former Senior Manager and Amazon Web Services acknowledged that he actually turns off his Alexa devices to prevent private conversations from being shared:

NARRATOR:

Once the device is awake and the blue light is on, it's recording.
And last year, it was revealed that Amazon employs thousands of

CLASS ACTION COMPLAINT - 15

people around the world to listen and transcribe some of those recordings to help train the system.

JAMES JACOBY [Correspondent]:

Do you think that you did a good enough job of disclosing that to consumers? That there are humans involved in listening to these recordings?

DAVE LIMP [Amazon Senior Vice President, Devices & Services]:

We try to articulate what we're doing with our products as clearly as we can. But if I could go back in time and I could be more clear and the team could be more clear on how we were using human beings to annotate a small percentage of the data, I would, for sure. What I would say, though, is that once we realize that customers didn't clearly understand this, within a couple of days we added an opt-out feature so that customers could turn off annotation if they so chose. And then within a month or two later we allowed people to auto-delete data, which they also asked for within that time frame.

We're not going to always be perfect, but when we make mistakes, I think the key is that we correct them very quickly on behalf of customers.

NARRATOR:

But even one of the founders of Amazon Web Services approaches his Alexa devices with caution.

JAMES JACOBY:

When do you turn off your Alexa?

ROBERT FREDERICK, Former senior manager, Amazon Web Services:

I turn off my Alexa when I know for a fact that the conversation that I am going to have or whenever I just want to have a private moment. I don't want certain conversations to be heard by humans, conversations that I know for a fact are not things that

CLASS ACTION COMPLAINT - 16

should be shared, then I actually turn off those particular listening devices.[19]

Plaintiff's Experience

66.   Plaintiff is an Amazon Prime member who owns an Amazon Echo equipped with Alexa services.

67.   On numerous occasions during the Class Period, Plaintiff, an Illinois citizen, spoke to her Alexa device located in her home in Illinois.

68.   After Plaintiff spoke into the Alexa device, Amazon collected, captured, received through trade, or otherwise obtained and disclosed Plaintiff's voiceprint and transcription thereof.

69.   Amazon did not obtain written releases from Plaintiff before capturing, collecting, receiving through trade, or otherwise obtaining her biometric identifiers or biometric information in compliance with 740 ILCS 14/15(b)(3).

70.   On certain occasions, Plaintiff's Alexa device would also light up when Plaintiff spoke words other than the "wake-word."

71.   Plaintiff's voiceprints are "biometric identifiers" pursuant to 740 ILCS 14/10.

72.   Transcripts of Plaintiff's voice recordings, which are derived from biometric identifiers, are "biometric information" pursuant to 740 ILCS 14/10.

73.   Any other data in Amazon's possession that links Plaintiff's voiceprints to Plaintiff also constitutes "biometric information" pursuant to 740 ILCS 14/10.

74.   As set forth herein, Amazon obtained the biometric identifiers and/or biometric information of Plaintiff and the Class in violation of BIPA.

---

[19] PBS Frontline.

CLASS ACTION COMPLAINT - 17

75.   Amazon's failures to comply with BIPA as set forth herein violated Plaintiff and the Class Members' privacy rights, and the harm to Plaintiff and the Class occurred in Illinois. *See Cothron*, 477 F. Supp.3d at 732 n.7 ("[T]he privacy concerns are implicated equally whether the new data is sent off-site for comparison or the old data is retrieved from an off-site location so that the comparison can take place on-site."); *In re Facebook Biometric Info. Privacy Litig.*, 326 F.R.D. 535, 547–48 (N.D. Cal. 2018) ("None of the class members are non-residents suing under Illinois law . . . . Contrary to Facebook's suggestion, the geographic location of its data servers is not a dispositive factor. The functionality and reach of modern online services like Facebook's cannot be compartmentalized into neat geographic boxes. Making the geographic coordinates of a server the most important circumstance in fixing the location of an Internet company's conduct would yield the questionable results *Avery* [*v. State Farm Mut. Auto. Ins. Co.*, 216 Ill.2d 100, 185 (Ill. 2005)] counsels against. Among other problematic outcomes, it would effectively gut the ability of states without server sites to apply their consumer protection laws to residents for online activity that occurred substantially within their borders. [Citation.] Correlatively, a single-minded focus on server location would also potentially nationalize the consumer protection laws of states that host servers, which in this case includes California. Both outcomes are fraught with unintended and undesirable consequences.").

CLASS ACTION ALLEGATIONS

76.   Plaintiff brings this class action on behalf of herself and all others similarly situated, as representative of the following class (the "Class"):

> All Illinois residents: (a) who own an Amazon Alexa device; and (b) from whom Amazon obtained a voice recording from an Amazon Alexa device located in Illinois during the Class Period.

CLASS ACTION COMPLAINT - 18

77.   Excluded from the Class are any Defendants, its parents, subsidiaries, affiliates, predecessors, successors, officers, directors, and the immediate family members of such persons. Also excluded are any trial judge who may preside over this action, court personnel and their family members and any juror assigned to this action.

78.   Plaintiff reserves the right to amend or modify the Class definitions with greater specificity or division into subclassses after having had an opportunity to conduct discovery.

79.   The Class Period is that period within the statute of limitations for this action and extending until a Class is certified herein.

80.   The Class is certifiable under Fed. R. Civ. P. 23.

81.   **Numerosity.** The members of the Class are so numerous that joinder of all members is impracticable. The determination of the numerosity factor can be made from Defendants' records.

82.   **Typicality.** Plaintiff's claims are typical of the claims of the Class Members. Plaintiff and all Class Members have had their rights under BIPA violated based on Amazon's failure to comply with the provisions of BIPA.

83.   **Commonality and Predominance**. There are questions of law and fact common to the Class, which predominate over any questions affecting individual members of the Class. These common questions of law and fact include, without limitation:

     a.   Whether Amazon collected, captured, received through trade, or otherwise obtained biometric identifiers or biometric information of Plaintiff and the Class;

     b.   Whether Amazon developed, made available to the public and complied with a retention and destruction policy in compliance with 740 ILCS 14/15(a);

CLASS ACTION COMPLAINT - 19

c. Whether Amazon informed Plaintiff and the Class in writing that it was collecting their biometric identifier or biometric information in compliance with 740 ILCS 14/15(b)(1);

d. Whether Amazon informed Plaintiff and the Class in writing of the specific purpose and length of term for which it was collecting their biometric identifier or biometric information in compliance with 740 ILCS 14/15(b)(2);

e. Whether Amazon received written releases executed by Plaintiff and the Class before capturing, collecting, receiving through trade, or otherwise obtaining their biometric identifiers or biometric information in compliance with 740 ILCS 14/15(b)(3);

f. Whether Amazon sold, leased, traded, or otherwise profited from the biometric identifier or biometric information of Plaintiff and the Class;

g. Whether Amazon disclosed, redisclosed, or otherwise disseminated the biometric identifier or biometric information of Plaintiff and the Class and whether such disclosure, redisclosure, or dissemination was in compliance with 740 ILCS 14/15(d)(1)-(4);

h. Whether Amazon stored, transmitted, and protected from disclosure all biometric identifiers and biometric information of Plaintiff and the Class using the reasonable standard of care within the industry in compliance with 740 ILCS 14/15(e)(1);

i. Whether Amazon stored, transmitted, and protected from disclosure all biometric identifiers and biometric information of Plaintiff and the Class in a manner that is the same as or more protective than the manner in which it stores, transmits, and protects other confidential and sensitive information in compliance with 740 ILCS 14/15(e)(2); and/or

j. Whether any violations of BIPA by Amazon were reckless, intentional, or negligent.

84. **Adequacy**. Plaintiff is a member of the Class she seeks to represent, is committed to the vigorous prosecution of this action, and has retained competent counsel experienced in the prosecution of class actions. Accordingly, Plaintiff is an adequate representative and will fairly and adeuately protect the interests of the Class.

CLASS ACTION COMPLAINT - 20

85.   **Superiority.** A class action is an appropriate method for the fair and efficient adjudication of this controversy and is superior to all other available methods. Because the amount of each individual Class member's claim is small relative to the complexity of the litigation, and due to the financial resources of Defendants, no Class member could afford to seek legal redress individually for the claims alleged herein. Therefore, absent a class action, Class members will continue to suffer losses and Defendants' misconduct will proceed without remedy. Even if Class members could afford such individual litigation, the court system could not. Given the complex legal and factual issues involved, individualized litigation would significantly increase the delay and expense to all parties and to the Court. Individualized litigation would also create the potential for inconsistent or contradictory rulings. By contrast, a class action presents far fewer management difficulties, allows claims to be heard that might otherwise go unheard because of the relative expense of bringing individual lawsuits, and provides the benefits of adjudication, economies of scale, and comprehensive supervision by a single court. Finally, Plaintiff knows of no difficulty that will be encountered in the management of this litigation that would preclude its maintenance as a class action.

86.   **Class Action on Limited Issues.** Because there are common individual issues among the Class, it is appropriate for this action to be maintained as a class action with respect to particular issues if necessary. *See* Fed. R. Civ. P. 23(c)(4).

CLAIMS FOR RELIEF

COUNT I

Amazon's Violations of the Biometric Information Privacy Act, 740 ILCS 14/15(a)

87.   Plaintiff incorporates by reference each and every allegation set forth above.

88.   Amazon qualifies as a "private entity" under BIPA. 740 ILCS 14/10.

CLASS ACTION COMPLAINT - 21

1

2

3

89.   On numerous occasions during the Class Period, Amazon has collected, captured, received through trade, or otherwise obtained Plaintiff's and the Class Members' voiceprints and transcriptions thereof.

4

5

6

7

8

9

10

90.   For some or all of the Class Period, Amazon did not develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information to occur by the earlier of: (a) when the original purpose for collecting or obtaining such identifiers has been satisfied, or (b) within 3 years of the individual's last interaction with the private entity, as required by 740 ILCS 14/15(a).

11

12

13

14

15

91.   To the extent Amazon has had such a retention and destruction policy in place that complies with BIPA, its failure to permanently delete Plaintiff and the Class' biometric identifiers and/or biometric information in compliance with such policy constitutes a violation of 740 ILCS 14/15(a).

16

17

92.   In violating BIPA, a law in effect since 2008, Amazon acted, and continues to act, recklessly and/or intentionally. At the least, Amazon negligently violated BIPA.

18

19

20

93.   Plaintiff and the Class Members are "aggrieved" under BIPA based on Amazon's violation of their rights under BIPA, and accordingly are entitled to seek damages and relief provided for under the statute. *See Rosenbach*, 2019 IL 123186, ¶ 40.

21

22

23

24

25

94.   Plaintiff and the Class Members seek, *inter alia*, statutory damages of $5,000 per intentional or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), statutory damages of $1,000 per negligent violation of BIPA pursuant to 740 ILCS 14/20(1), and reasonable attorneys' fees and costs pursuant to 740 ILCS 14/20(3).

26

CLASS ACTION COMPLAINT - 22

1
2

WHEREFORE, Plaintiff and the Class pray for the relief requested in the Prayer for Relief set forth below.

COUNT II

Amazon's Violations of the Biometric Information Privacy Act, 740 ILCS 14/15(b)

95.   Plaintiff incorporates by reference each and every allegation set forth above.

96.   Plaintiff and the Class did not execute a written release related to Amazon's collection, capturing, purchasing, receiving through trade, or otherwise obtaining their voiceprints, transcriptions thereof, or other biometric information derived from the voiceprints.

97.   For some or all of the Class Period, Amazon did not properly inform Plaintiff and the Class in writing that their biometric identifiers and/or biometric information was being collected and/or stored, nor did it inform them in writing of the specific purpose and length of term for which their biometric identifiers and/or biometric information was being collected, stored, and used as required by 740 ILCS 14/15(b)(1)-(2).

98.   For some or all of the Class Period, Amazon systematically and intentionally collected, obtained, used, and/or stored the biometric identifiers and/or biometric information of Plaintiff and the Class without first obtaining from Plaintiff and the Class Members the specific executed written release required by 740 ILCS 14/15(b)(3).

99.   In violating BIPA, a law in effect since 2008, Amazon acted, and continues to act, recklessly and/or intentionally. At the least, Amazon negligently violated BIPA.

100.   Plaintiff and the Class Members are "aggrieved" under BIPA based on Amazon's violation of their rights under BIPA, and accordingly are entitled to seek damages and relief provided for under the statute. *See Rosenbach*, 2019 IL 123186, ¶ 40.

CLASS ACTION COMPLAINT - 23

1   101.   Plaintiff and the Class Members seek, *inter alia*, statutory damages of $5,000

2   per intentional or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), statutory damages

3   of $1,000 per negligent violation of BIPA pursuant to 740 ILCS 14/20(1), and reasonable

4   attorneys' fees and costs pursuant to 740 ILCS 14/20(3).

5   WHEREFORE, Plaintiff and the Class pray for the relief requested in the Prayer for

6   Relief set forth below.

7
                                    COUNT III
8
    Amazon's Violations of the Biometric Information Privacy Act, 740 ILCS 14/15(c)
9
        102.   Plaintiff incorporates by reference each and every allegation set forth above.
10
        103.   As set forth above, for some or all of the Class Period, Amazon used the
11
12 biometric identifiers and/or biometric information of Plaintiff and the Class to improve Alexa's

13 natural language understanding and for its own commercial purposes.

14   104.   Amazon's use of the biometric identifiers and biometric information of Plaintiff

15 and the Class to improve Alexa's natural language understanding, expand the scope of Alexa
16
    products, and create other business opportunities for Amazon has benefited Amazon through
17
18 increased sales of its improved voice-recognition products.

19   105.   For instance, Amazon has utilized the biometric identifiers and/or biometric data

20 to make Alexa compatible with over 100,000 products. Without the identified biometric data,

21
    there would be fewer, and worse-functioning Alexa products for Amazon to profit from.
22
        106.   Moreover, Amazon has profited from linking the voiceprints in their possession
23
24 to Plaintiff and the Class's accounts and other activities involving Amazon.

25   107.   As Shoshanna Zuboff, author of "The Age of Surveillance Capitalism," puts it:

26 "[Amazon] is going to know more about you than anyone knows. They're trying to move as

CLASS ACTION COMPLAINT - 24

intimately as possible and as quietly as possible into everyday life. Amazon wants to have the entire environment essentially miked. They want your walk in the park, they want your run down the city street. They want what you do in your car, they [want] what you do in your home. All these intimacies, all this insight is being integrated—analyzed and integrated. That is an extraordinary kind of power that has never existed before."[20]

108.   Furthermore, Amazon has used the biometric identifiers and biometric information of Plaintiff and the Class to create technology that is so intertwined with the biometric data that marketing the Alexa technology is essentially disseminating biometric data for profit.

109.   Additionally, Amazon has used the biometric identifiers and biometric information of Plaintiff and the Class to obtain a competitive advantage over other businesses offering similar devices that provide similar voice-based services as Amazon.

110.   Accordingly, Amazon violated 740 ILCS 14/15(c) by selling, leasing, trading, or otherwise profiting from Plaintiff's and Class Members' biometric identifiers and/or biometric information in its possession.

111.   In violating BIPA, a law in effect since 2008, Amazon acted, and continues to act, recklessly and/or intentionally. At the least, Amazon negligently violated BIPA.

112.   Plaintiff and the Class Members are "aggrieved" under BIPA based on Amazon's violation of their rights under BIPA, and accordingly are entitled to seek damages and relief provided for under the statute. *See Rosenbach*, 2019 IL 123186, ¶ 40.

113.   Plaintiff and the Class Members seek, *inter alia*, statutory damages of $5,000 per intentional or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), statutory damages

---

[20] PBS Frontline.

CLASS ACTION COMPLAINT - 25

of $1,000 per negligent violation of BIPA pursuant to 740 ILCS 14/20(1), and reasonable

attorneys' fees and costs pursuant to 740 ILCS 14/20(3).

WHEREFORE, Plaintiff and the Class pray for the relief requested in the Prayer for

Relief set forth below.

COUNT IV

Amazon's Violations of the Biometric Information Privacy Act, 740 ILCS 14/15(d)

114. Plaintiff incorporates by reference each and every allegation set forth above.

115. As set forth above, Amazon employs thousands of individuals around the world,

including both full-time Amazon employees and third-party contractors, who have access to

and listen to voiceprints and review the transcriptions captured by Amazon's devices.

116. Thus, for some or all of the Class Period, Amazon disclosed, redisclosed, or

otherwise disseminated Plaintiff's and the Class Members' biometric identifiers and

information to third parties.

117. Amazon's disclosed, redisclosed, or disseminated Plaintiff's and the Class

Members' biometric identifiers and information without satisfying the requirements of 740

ILCS 14/15(d). Specifically, Amazon has never informed nor received consent from Plaintiff

or the Class Members to disclose and/or redisclose their biometric identifiers and biometric

information to third parties; the disclosure or redisclosure did not complete a financial

transaction authorized by the subject; and the disclosure or redisclosure was not required by

law or pursuant to a valid warrant or subpoena.

118. In violating BIPA, a law in effect since 2008, Amazon acted, and continues to

act, recklessly and/or intentionally. At the least, Amazon negligently violated BIPA.

CLASS ACTION COMPLAINT - 26

119.   Plaintiff and the Class Members are "aggrieved" under BIPA based on Amazon's violation of their rights under BIPA, and accordingly are entitled to seek damages and relief provided for under the statute. *See Rosenbach*, 2019 IL 123186, ¶ 40.

120.   Plaintiff and the Class Members seek, *inter alia*, statutory damages of $5,000 per intentional or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), statutory damages of $1,000 per negligent violation of BIPA pursuant to 740 ILCS 14/20(1), and reasonable attorneys' fees and costs pursuant to 740 ILCS 14/20(3).

WHEREFORE, Plaintiff and the Class pray for the relief requested in the Prayer for Relief set forth below.

COUNT V

Amazon's Violations of the Biometric Information Privacy Act, 740 ILCS 14/15(e)

121.   Plaintiff incorporates by reference each and every allegation set forth above.

122.   For some or all of the Class Period, Amazon has failed to store, transmit, and protect from disclosure the biometric identifiers and/or biometric information of Plaintiff and the Class using the reasonable standard of care within the industry, in violation of 740 ILCS 14/15(e)(1).

123.   Additionally, for some or all of the Class Period, Amazon has failed to store, transmit, and protect from disclosure the biometric identifiers and/or biometric information of Plaintiff and the Class in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

124.   For example, as set forth above, Amazon permits its employees and third-party contractors to disseminate biometric data simply because they find it "amusing."

CLASS ACTION COMPLAINT - 27

125.   In violating BIPA, a law in effect since 2008, Amazon acted, and continues to

act, recklessly and/or intentionally. At the least, Amazon negligently violated BIPA.

126.   Plaintiff and the Class Members are "aggrieved" under BIPA based on

Amazon's violation of their rights under BIPA, and accordingly are entitled to seek damages

and relief provided for under the statute. *See Rosenbach*, 2019 IL 123186, ¶ 40.

127.   Plaintiff and the Class Members seek, *inter alia*, statutory damages of $5,000

per intentional or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), statutory damages

of $1,000 per negligent violation of BIPA pursuant to 740 ILCS 14/20(1), and reasonable

attorneys' fees and costs pursuant to 740 ILCS 14/20(3).

WHEREFORE, Plaintiff and the Class pray for the relief requested in the Prayer for

Relief set forth below.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class, pray for judgment against

Defendants as follows:

A.   entering an order certifying the Class as requested herein and appointing

the undersigned as lead counsel for the Class;

B.   awarding statutory damages of $5,000 for each willful and/or reckless

violation of BIPA pursuant to 740 ILCS 14/20(2), or, in the alternative,

statutory damages of $1,000 for each negligent violation of BIPA

pursuant to 740 ILCS 14/20(1);

C.   enjoining Amazon from collecting, obtaining, storing, using, selling,

leasing, trading, profiting from, disclosing, redisclosing, or otherwise

CLASS ACTION COMPLAINT - 28

disseminating Plaintiff's and the Class's biometric identifiers until done so in compliance with BIPA;

D.   awarding Plaintiff her reasonable attorneys' fees, costs, and other expenses pursuant to 740 ILCS 14/20(3);

E.   awarding Plaintiff pre-judgment and post-judgment interest, as provided by law; and

F.   awarding such other and further relief as is just and appropriate.

JURY DEMAND

Plaintiff demands a trial by jury on all claims so triable.

Dated this 9th day of July, 2021.   Respectfully submitted,

TOUSLEY BRAIN STEPHENS PLLC

By: /s/ Jason T. Dennett
/s/ Cecily C. Shiel
Jason T. Dennett, WSBA #30686
jdennett@tousley.com
Cecily C. Shiel, WSBA #50061
cshiel@tousley.com
1700 Seventh Avenue, Suite 2200
Seattle, WA 98101-4416
Telephone: (206) 682-5600

Thomas P. Rosenfeld, *pro hac vice forthcoming*
Kevin P. Green, *pro hac vice forthcoming*
Zachary T. Shelton, *pro hac vice forthcoming*
**GOLDENBERG HELLER
& ANTOGNOLI, P.C.**
2227 South State Route 157
Edwardsville, IL 62025
(618) 656-5150
tom@ghalaw.com
kevin@ghalaw.com
zachary@ghalaw.com

CLASS ACTION COMPLAINT - 29

1	James P. Frickleton, *pro hac vice forthcoming*
	Edward D. Robertson, Jr., *pro hac vice forthcoming*
2	Edward D. Robertson III, *pro hac vice forthcoming*
3	**BARTIMUS FRICKLETON**
	ROBERTSON RADER, P.C.
4	4000 W. 114th St., Suite 310
	Leawood, KS 66211
5	(913) 266-2300/ Fax (913) 266-2366
6	jimf@bflawfirm.com
	chiprob@bflawfirm.com
7	krobertson@bflawfirm.com
8	
9	***Attorneys for Plaintiff***

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

CLASS ACTION COMPLAINT - 30

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Amazon's Collection of Alexa Users' Voice Recordings Violates Ill. Privacy Law, Class Action Alleges](#)