

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

**RODNEKA PERRY, individually, and on )  
behalf of all others similarly situated, )**

**Plaintiff, )**

**v. )**

**AMAZON LOGISTICS, INC., )  
AMAZON.COM, INC., AMAZON.COM )  
SERVICES, LLC f/k/a AMAZON.COM, )  
LLC, and AMAZON WEB SERVICES, INC. )**

**Defendants. )**

**Case No 2023CH03680**

**CLASS ACTION COMPLAINT**

Plaintiff Rodneka Perry (“Plaintiff”), individually and on behalf of all others similarly situated (the “Class”), brings the following Class Action Complaint (“Complaint”) pursuant to the Illinois Code of Civil Procedure, 735 ILCS §§ 5/2-801 and 2-802 and against (1) Amazon Logistics, Inc., (2) Amazon.com, Inc., (3) Amazon.com Services, LLC f/k/a Amazon.com, LLC, and, (4) Amazon Web Services, Inc. (“AWS”), collectively, (“Amazon” or “Defendants”) to redress and curtail each Defendant’s unlawful collection, use, storage, and disclosure of Plaintiff’s and other similarly situated individuals’ sensitive and proprietary biometric identifiers and biometric information (“biometric data”). Plaintiff alleges as follows upon personal knowledge as to herself, her own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by her attorneys.

**NATURE OF THE ACTION**

1. Amazon.com, Inc. and Amazon.com Services, LLC, commonly known as “Amazon,” is a leading multinational technology company, specializing in e-commerce, cloud-

FILED DATE: 4/17/2023 10:26 AM 2023CH03680

based servicing, streaming and artificial intelligence. It is considered one of the “Big Four” technology companies, alongside Google, Apple, and Facebook.

2. Amazon Logistics, Inc., is a subsidiary of Amazon.com, Inc. and provides the fulfillment and delivery infrastructure for Amazon.com, Inc. through applications, including, but not limited to Amazon Flex. Amazon Flex is a job service platform with a corresponding application that provides an opportunity for independent contractors to accept assignments and deliver packages on behalf of Amazon Logistics, Inc. or Amazon.com, Inc. using their own vehicles.

3. AWS is a subsidiary of Amazon.com, Inc. and one of the largest platforms and providers for cloud computing services.

4. In September 2018, Named Plaintiff, Rodneka Perry, downloaded the Amazon Flex application, created an account, and started work as a delivery driver in the Greater Chicago area and continues to do so until the present.

5. Through Amazon Flex, Plaintiff accepts jobs and delivers Amazon packages, Prime Now household items, and Amazon Fresh groceries to customers in the Greater Chicago area using her own vehicle.

6. In mid-2019 Amazon Flex installed a feature where, before Plaintiff or anyone else can accept work and start delivering packages, the user is required to scan his or her face using their mobile device for identity verification purposes.

7. Any Amazon Flex user, including Plaintiff, must have their facial geometry collected and stored by Amazon as a requirement for them to deliver Amazon’s packages.

8. Amazon Flex admits as much in the FAQ section of its application where it states:

“To use the Amazon delivery application, Amazon requires that users provide a photo to help us identify them. Using this photo, we may create a facial scan or similar biometric identifier, which we refer to as ‘Biometric Information.’”<sup>1</sup>

9. However, Amazon fails to secure Amazon Flex users’ informed written consent before collecting, storing, and disseminating their biometric identifiers and biometric information.

10. Since approximately 2016, Amazon has been using Artificial Intelligence (“AI”) machine-learning image and video recognition systems, including Amazon Rekognition.

11. Rekognition is an image-recognition technology that Amazon uses itself and markets and sells to businesses, governmental entities, and other third parties through AWS. According to AWS’s own FAQ, the most common use cases for Rekognition include: “Searchable Image Library, Face-Based User Verification, Sentiment Analysis, Facial Recognition, and Image Moderation.”<sup>2</sup>

12. Amazon captures the image data of Plaintiff and other Illinois Amazon Flex users which are then shared with Amazon software programs, including but not limited to Rekognition, to identify and detect and to enhance their own systems and technology, including the Rekognition system itself.

13. Upon information and belief, Amazon requires its Amazon Flex users to take and upload pictures of themselves into the application and uses associated facial recognition software, including but not limited to Rekognition, in order to verify the users’ identities before allowing them to proceed with their Amazon Flex shift.

14. Defendant AWS’s associated facial recognition software collects and captures, stores and uses biometric identifiers, namely scans of an individual’s facial geometry.

---

<sup>1</sup> *Amazon Flex – FAQs* (last visited April 14, 2023), <https://flex.amazon.com/faq>

<sup>2</sup> *Amazon Rekognition – FAQs* (last visited July 21, 2022), <https://aws.amazon.com/rekognition/faqs/?nc=sn&loc=7>

15. Facial geometry and other biometrics are unique and personal identifiers that cannot be changed. 740 ILCS § 14/5(c).

16. Critically, it is unclear how long each Defendant retains the biometric identifiers and information derived from the capturing of Plaintiff's and other Amazon Flex users' faces.

17. Recognizing the need to protect its citizens' right of control over their biometric data, Illinois enacted the Biometric Information Privacy Act ("BIPA"), 740 ILCS § 14/1, *et seq.*, specifically to regulate companies that collect, store, and use Illinois citizens' biometrics, such as facial geometry scans. 740 ILCS § 14/5.

18. Notwithstanding the clear and unequivocal requirements of the law, Amazon knowingly disregards Plaintiff's and other similarly situated users' statutorily protected privacy rights and unlawfully collects, obtains, stores, disseminates, and uses Plaintiff's and other similarly situated users' biometric data in violation of BIPA. Specifically, Defendants violated and continue to violate BIPA because they did not and continue not to:

- a. Properly or adequately inform Plaintiff and others similarly situated in writing that biometric identifiers or biometric information are being collected, obtained or stored, as required by BIPA;
- b. Properly or adequately inform Plaintiff and others similarly situated in writing of the specific purpose and length of time for which her facial scans and other biometric identifiers or biometric information were being collected, obtained, stored, and used, as required by BIPA;
- c. Develop and adhere to a BIPA-compliant publicly available retention schedule and guidelines for permanently destroying Plaintiff's and others similarly situated facial scans and other biometric identifiers or biometric information, as required by BIPA;
- d. Obtain a written release from Plaintiff and others similarly situated to collect, obtain, capture, or otherwise obtain their facial scans and other biometric identifiers or biometric information, as required by BIPA; and,

- e. Obtain consent from Plaintiff and others similarly situated to disclose, redisclose, or otherwise disseminate their facial scans and other biometric identifiers or biometric information to a third party, as required by BIPA.

19. Accordingly, Plaintiff, on behalf of themselves as well as the putative Class, seeks an Order: (1) declaring that Amazon’s conduct violates BIPA; (2) requiring Amazon to cease the unlawful activities discussed herein; and (3) awarding statutory damages to Plaintiff and the putative Class.

**PARTIES**

20. Plaintiff Rodneka Perry is a natural person and at all relevant times was a resident of the State of Illinois.

21. Defendant Amazon.com, Inc. is a Delaware corporation that is registered to do business in Illinois.

22. Defendant Amazon.com Services, LLC is a Delaware corporation that is registered to do business in Illinois.

23. Defendant Amazon Web Services, Inc. is a Delaware corporation that is registered to do business in Illinois.

24. Defendant Amazon Logistics, Inc. is a Delaware corporation that is registered to do business in Illinois.

**JURISDICTION AND VENUE**

25. This Court has jurisdiction over each Defendant pursuant to 735 ILCS § 5/2-209 because each Defendant conducts business in Illinois, has locations in Illinois, and committed statutory violations alleged herein in Cook County, Illinois.

26. Venue is proper in Cook County because each Defendant conducts business in Cook County and committed statutory violations alleged herein in Cook County, Illinois.

## FACTUAL BACKGROUND

### I. The Biometric Information Privacy Act.

27. In the early 2000s, major national corporations started using Chicago and other locations in Illinois to test “new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias.” 740 ILCS § 14/5(c). Given its relative infancy, an overwhelming portion of the public became weary [sic] of this then-growing yet unregulated technology. *See* 740 ILCS § 14/5.

28. In late 2007, a biometrics company called Pay by Touch, which provided major retailers throughout the State of Illinois with fingerprint scanners to facilitate consumer transactions—including at retail grocery stores—filed for bankruptcy. That bankruptcy alarmed the Illinois Legislature because suddenly there was a serious risk that millions of fingerprint records—which, like other unique biometric identifiers, can be linked to people’s sensitive financial and personal data—could now be sold, distributed, or otherwise shared through the bankruptcy proceedings to third parties without adequate protections for Illinois citizens. The bankruptcy also highlighted the fact that most consumers who used the company’s fingerprint scanners were completely unaware the scanners were not actually transmitting fingerprint data to the retailer who deployed the scanner, but rather to Pay by Touch, and that their unique biometric identifiers could now be sold to unknown third parties. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276, p. 249.

29. Recognizing the “very serious need [for] protections for the citizens of Illinois when it [came to their] biometric information,” Illinois enacted BIPA in 2008. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276; 740 ILCS § 14/5.

30. Additionally, to ensure compliance, BIPA provides that, for each violation, the prevailing party may recover \$1,000 or actual damages, whichever is greater, for negligent violations and \$5,000, or actual damages, whichever is greater, for intentional or reckless violations. 740 ILCS § 14/20.

31. BIPA is an informed consent statute that achieves its goal by making it unlawful for a company to, among other things, collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it first:

- a. Informs the subject in writing that a biometric identifier or biometric information is being collected, obtained, stored, and used;
- b. Informs the subject in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, obtained, stored, and used; and
- c. Receives a written release executed by the subject of the biometric identifier or biometric information.

*See* 740 ILCS § 14/15(b).

32. Biometric identifiers include facial scans, retina and iris scans, voiceprints, scans of hands, and fingerprints. *See* 740 ILCS § 14/10. Biometric information is defined separately to include any information based on an individual's biometric identifier that is used to identify an individual. *Id.*

33. BIPA establishes standards for how companies must handle biometric identifiers and biometric information. *See, e.g.,* 740 ILCS § 14/15(c)-(d). For example, BIPA prohibits private entities from disclosing a person's or customer's biometric identifier or biometric information without first obtaining consent for such disclosure. *See* 740 ILCS § 14/15(d)(1).

34. BIPA requires companies to develop and comply with 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 such identifiers or information has been satisfied, or within three years of the individual’s last interaction with the company, whichever occurs first. 740 ILCS § 14/15(a).

35. The Illinois legislature enacted BIPA due to the increasing use of biometric data in financial and security settings, the general public’s hesitation to use biometric information, and—significantly—the unknown ramifications of biometric technology. Biometrics are biologically unique to the individual and, once compromised, an individual is at a heightened risk for identity theft and left without any recourse. 740 ILCS § 14/5.

36. BIPA provides individuals with a private right of action, protecting their right to privacy regarding their biometrics as well as protecting their rights to know the precise nature for which their biometrics are used and how they are being stored and ultimately destroyed. Unlike other statutes that only create a right of action if there is a qualifying data breach, BIPA strictly regulates the manner in which entities may collect, store, use, and disseminate biometrics and creates a private right of action for lack of statutory compliance. 740 ILCS § 14/20.

37. Plaintiff, like the Illinois legislature, recognizes how imperative it is to keep biometric information secure. Biometric information, unlike other personal identifiers such as a social security number, cannot be changed or replaced if hacked or stolen.

## **II. Amazon Violates the Biometric Information Privacy Act.**

38. Each Defendant failed to take note of the shift in Illinois law governing the collection, use, storage, and dissemination of biometric data and continues to collect, store, use, and disseminate Amazon Flex users’ biometric data in violation of BIPA.



39. In 2019, Amazon faced a similar lawsuit alleging that Amazon’s “Alexa” devices retained minor users’ voice prints and information without proper consent in violation of BIPA. There, Amazon was accused by guardians of minors of unlawful collection, use, storage and disclosure of minor users’ biometric data through the use of its “Alexa” devices and voice printing system. Between 2019 – 2023, at least twenty other similar lawsuits have since been brought against Amazon entities, including AWS, alleging BIPA violations from their improper collection of individuals’ biometric identifiers and information and their improper use of said data to train and enhance Rekognition.<sup>3</sup>

---

<sup>3</sup> See *Trio v. Amazon Web Services, Inc.*, Case No 1:23-CV-01389, filed March 6, 2023, in the Northern District of Illinois (removed from the Circuit Court of Cook County Illinois, Case No. 2023-CH-00544); See *Redd v. Amazon Web Services, Inc.*, Case No. 1:22-CV-06779, filed Dec. 2, 2022, in the Northern District of Illinois (removed from the Circuit Court of Cook County, Illinois, with Case No. 2022-CH-08721); See *Dorian v. Amazon Web Services, Inc.*, Case No. 2:22-CV-00269, filed March 7, 2022, in the Western District of Washington; See *Reid v. Amazon.com, Inc. et al.*, Case No. 1:21-CV-06010, filed Nov. 9, 2021, in the Northern District of Illinois; See *Mayhall v. Amazon Web Services, Inc. et al.*, Case No. 2:21-CV-04173, filed Oct. 29, 2021, in the Western District of Washington; See *Svoboda v. Amazon, Inc., et al.*, Case No. 1:21-CV-05336, filed Oct. 7, 2021, in the Northern District of Illinois (removed from the Circuit Court of Cook County, Illinois, with Case No. 2021-CH-04516); See *Schaeffer v. Amazon.com, Inc. et al.*, Case No. 3:21-CV-01080, filed Aug. 31, 2021, in the Southern District of Illinois (removed from the Circuit Court of Madison County, Illinois, under Case No. 2021-C-000876); See *Flores et al., v. Amazon, Inc. et al.*, Case No. 1:21-CV-04064, filed Aug. 2, 2021, in the Northern District of Illinois (case in other court: Washington Western, 2:21-CV-00873); *Cooper v. Amazon, Inc. et al.*, Case No. 2:21-CV-00915, filed Jul. 8, 2021, in the Western District of Washington (electronically transferred on Aug. 30, 2021, to the Northern District of Illinois, as Case No. 1:21-CV-04633); See *B.H. v. Amazon.com, Inc.*, Case No. 1:21-CV-03169, filed Jun. 11, 2021, in the Northern District of Illinois (removed from the Circuit Court of Cook County, Illinois, Case No. 2021-CH-02330); See *Rosati v. Amazon.com, Inc.*, Case No. 2:21-CV-00409, filed March 26, 2021, in the Western District of Washington (removed from the Superior Court of Washington for King County, Case No. 21-2-03591 SEA); See *Bond v. Amazon, Inc.*, Case No. 1:21-CV-01578, filed Jan. 28, 2021, in the 16th Judicial Circuit Court, Kane County, Illinois; See *Jerinic v. Amazon.com, Inc.*, Case No. 1:20-CV-06485, filed Oct. 20, 2020, in the Northern District of Illinois (removed from the Circuit Court of Cook County, Illinois, Case No. 2020-CH-06036); See *Vance v. Amazon.com, Inc.*, Case No. 2:20-CV-01084, filed July 14, 2020, in the Western District of Washington; See *Ragsdale v. Amazon Web Services, Inc.*, Case No. 1:20-CV-00560, filed Jan. 24, 2020, in the Northern District of Illinois (removed from the Circuit Court of Cook County, Illinois, case no. 2109-CH-013251); See *McGoveran v. Amazon Web Services, Inc.* Case No. 3:20-CV-00031, filed Jan. 8, 2020, in the Southern District of Illinois (removed from the Circuit Court of Madison County, Illinois, Case No. 2019-L-001786) (*McGoveran et al v. Amazon Web Services, Inc. et al.*, Case No. 1:20-CV-01399, filed Oct. 16, 2020, in the District of Delaware); See *Hryniewick v. Amazon Web Services, Inc.*, Case No. 1:19-CV-07569, filed Nov. 15, 2019, in the Northern District of Illinois (removed from the Circuit Court of Lake County, Illinois, Case No. 2019-CH-00001155); See *Adamsky et al v. Amazon.com, Inc. et al.*, Case No. 2:19-CV-01214, filed Aug. 2, 2019, in

40. Despite these prior accusations and all Defendants' knowledge of BIPA, here, Amazon captures and scans Amazon Flex users' biometric identifiers, particularly their facial geometry, through Amazon Flex's identity verification checks, and uploads and stores their data on Amazon's networked databases for use with Amazon's facial detection and recognition technology and software, including but not limited to Rekognition.

41. Amazon uses the biometric identifiers and information of Amazon Flex users from image data captured by Amazon Flex to identify users and to train and enhance the Rekognition system.

42. This is done through one of Rekognition's main features which is its ability to detect and analyze faces from still images or videos and compare them with other faces detected from other images. From these images, Rekognition can provide information including but not limited to "...facial landmarks such as the position of eyes, and detected emotions such as happy or sad."<sup>4</sup> Once an image containing a face is provided to Rekognition, it "detects the face in the image, analyzes the facial attributes of the face, and then returns a percent confidence score for the face and facial attributes that are detected in the image." See Figures 1 and 2 below, showing screenshots from Amazon's AWS Rekognition website and Developer Guide.

---

the Western District of Washington; See *Wilcosky v. Amazon.com, Inc. et al.*, Case No. 1:19-CV-05061, filed July 26, 2019, in the Northern District of Illinois (removed from the Circuit Court of Cook County, Illinois, Case No. 2019-CH-07777); See *Williams v. Inpax Shipping Solutions*, Case No. 2018-CH-02307, filed Feb. 21, 2018, in the Circuit Court of Cook County, Illinois.

<sup>4</sup> *Amazon Rekognition - Developer Guide* (last visited July 18, 2022), <https://docs.aws.amazon.com/rekognition/latest/dg/rekognition-dg.pdf#what-is>



### Face compare and search

Determine the similarity of a face against another picture or from your private image repository.

[Learn more »](#)



### Face detection and analysis

Detect faces appearing in images and videos and recognize attributes such as open eyes, glasses, and facial hair for each.

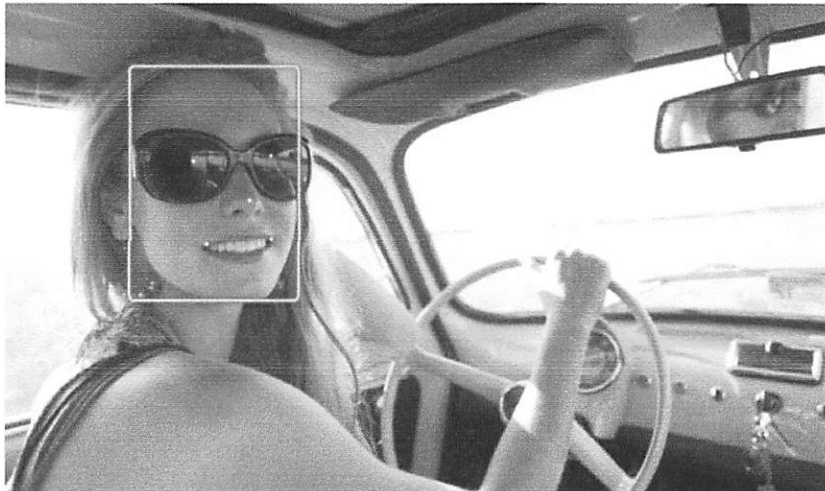
[Learn more »](#)

**(Figure 1.)**

## Detecting and analyzing faces

Amazon Rekognition can detect faces in images and videos. This section covers non-storage operations for analyzing faces. With Amazon Rekognition, you can get information about where faces are detected in an image or video, facial landmarks such as the position of eyes, and detected emotions (for example, appearing happy or sad). You can also compare a face in an image with faces detected in another image.

When you provide an image that contains a face, Amazon Rekognition detects the face in the image, analyzes the facial attributes of the face, and then returns a percent confidence score for the face and the facial attributes that are detected in the image.



**(Figure 2.)**

## Searching faces in a collection

Amazon Rekognition can store information about detected faces in server-side containers known as collections. You can use the facial information that's stored in a collection to search for known faces in images, stored videos, and streaming videos. Amazon Rekognition supports the `IndexFaces` operation. You can use this operation to detect faces in an image and persist information about facial features that are detected into a collection. This is an example of a *storage-based* API operation because the service persists information on the server.

To store facial information, you must first create (`CreateCollection`) a face collection in one of the AWS Regions in your account. You specify this face collection when you call the `IndexFaces` operation. After you create a face collection and store facial feature information for all faces, you can search the collection for face matches. To search for faces in an image, call `SearchFacesByImage`. To search for faces in a stored video, call `StartFaceSearch`. To search for faces in a streaming video, call `CreateStreamProcessor`.

### Note

The service doesn't persist actual image bytes. Instead, the underlying detection algorithm first detects the faces in the input image, extracts facial features into a feature vector for each face, and then stores it in the collection. Amazon Rekognition uses these feature vectors when performing face matches.

You can use collections in a variety of scenarios. For example, you might create a face collection to store scanned badge images by using the `IndexFaces` operation. When an employee enters the building, an image of the employee's face is captured and sent to the `SearchFacesByImage` operation. If the face match produces a sufficiently high similarity score (say 99%), you can authenticate the employee.

### (Figure 3.)

43. Rekognition is also able to store the information from these scans (“facial metadata”) into databases which it can search through to compare faces. *See* Figure 3 above, showing a screenshot from Amazon’s AWS Rekognition Developer Guide.

44. Each Defendant fails to adequately inform Amazon Flex users that it is collecting, obtaining or storing biometric data; fails to adequately inform Amazon Flex users of the specific purposes and duration for which it collects and obtains their sensitive biometric data and that the purpose of Amazon’s biometric data collection is to identify and detect users and to train Rekognition; fails to obtain written releases from Amazon Flex users before collecting or obtaining their sensitive biometric data; and fails to inform Amazon Flex users that it discloses their sensitive

- G. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and,
- H. Awarding such other and further relief as equity and justice may require.

Date: April 17, 2023

Respectfully Submitted,

/s/Mohammed A. Rathur

Ryan F. Stephan  
Catherine Mitchell  
Mohammed A. Rathur  
**STEPHAN ZOURAS, LLP**  
222 W. Adams Street, Suite 2020  
Chicago, Illinois 60606  
Telephone: (312) 233-1550  
Facsimile: (312) 233-1560  
Firm ID: 43734  
rstephan@stephanzouras.com  
cmitchell@stephanzouras.com  
mrathur@stephanzouras.com

*Counsel for Plaintiff and the Putative Class*