UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

JACINDA DORIAN, individually and on behalf of all others similarly situated, *Plaintiff*, *v.* AMAZON WEB SERVICES, INC., a Delaware corporation, *Defendant*.	Case No. CLASS ACTION COMPLAINT JURY DEMAND

Plaintiff Jacinda Dorian brings this Class Action Complaint and Demand for Jury Trial against Defendant Amazon Web Services, Inc. ("AWS") to put a stop to its surreptitious collection, use, and storage of Plaintiff's and the proposed Class's biometric data. Plaintiff alleges as follows upon personal knowledge as to herself and her own acts and experiences, and, as to all other matters, upon information and belief.

NATURE OF THE ACTION

1. Amazon.com, Inc. ("Amazon.com") is the world's largest online retailer and one of the largest providers of cloud computing services, called Amazon Web Services ("AWS").

2. According to Amazon.com, AWS is the world's most comprehensive and broadly adopted cloud platform, offering its customers over 200 cloud-based services from data centers globally. Millions of customers—from startups to the largest enterprises—use AWS every day.

3. One of AWS's services is a facial recognition program called Amazon

Rekognition. Rekognition uses machine vision and algorithmic classification techniques to map human facial geometry and analyze the resulting data to, for example, check whether two photographs depict the same individual.

4. Thousands of organizations use Amazon Rekognition to identify individuals using face recognition. In such circumstances, individuals' facial geometry is extracted by AWS and is stored not only by its customers on the cloud, but also by AWS on AWS's own servers.

5. However, because Rekognition is a behind-the-scenes service for businesses, consumers are largely unaware that when they use their favorite mobile app or online service to verify their identities, AWS is actually collecting and storing their biometric data.

6. Through these practices, AWS not only disregards individuals' privacy rights; it also violates the Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA"), which was specifically designed to protect Illinois residents from practices like Amazon's.

7. Accordingly, this Complaint seeks an order (i) declaring that AWS's conduct violates the BIPA; (ii) requiring AWS to cease the unlawful activities discussed herein; and (iii) awarding statutory damages to Plaintiff and the proposed Class (defined below).

PARTIES

8. Plaintiff Jacinda Dorian is a citizen and resident of the State of Illinois and has an intent to remain there, and is therefore a domiciliary of Illinois.

9. Defendant Amazon Web Services, Inc. is a Delaware corporation with its headquarters in Seattle, Washington. Amazon Web Services, Inc. is a subsidiary of Amazon.com, Inc. (Amazon Web Services, Inc. and Amazon.com, Inc. are collectively referred to as "Amazon," unless otherwise specified).

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction under 28 U.S.C. § 1332(d)(2) because (a) at least one member of the Class is a citizen of a state different from Defendant, (b) the amount in controversy exceeds $5,000,000, exclusive of interests and costs, and (c) none of the exceptions under that subsection apply to this action.

11. The Court has personal jurisdiction over Defendant because Defendant is licensed to conduct business in this District and maintains its headquarters and principal place of business in this District.

12. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant is licensed to conduct business in this District and its headquarters and principal place of business are maintained in this District.

FACTUAL ALLEGATIONS

I. The Use of Biometrics and Consumer Privacy.

13. "Biometrics" refer to technologies used to identify an individual based on unique physical characteristics. Common biometric identifiers include retina or iris scans, fingerprints, voiceprints, or hand or face geometry scans.

14. One of the most prevalent uses of biometrics is facial recognition technology, which works by scanning an image for human faces, extracting facial feature data from a photograph or image of a human face, generating a "faceprint" from the image through the use of facial recognition algorithms, and then comparing the resultant faceprint to other faceprints stored in a faceprint database. If a database match is found, a person may be identified.

15. Unlike other identifiers such as Social Security or credit card numbers, which can be changed if compromised or stolen, biometric identifiers linked to a specific voice or face cannot. These unique and permanent biometric identifiers, once exposed, leave victims with no means to prevent identity theft and unauthorized tracking. *See also* 740 ILCS 14/5(c).

II. Illinois's Biometric Information Privacy Act.

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

17. The BIPA is an informed consent statute which 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:

> (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or biometric information."

740 ILCS 14/15(b).

18. The BIPA also establishes standards for how companies must handle Illinois consumers' biometric identifiers and biometric information. *See, e.g.*, 740 ILCS 14/15(a), (c)–(d). For instance, the 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).

19. The BIPA also prohibits private entities from disclosing a person's or customer's biometric identifier or biometric information to third parties without first obtaining consent for that disclosure, 740 ILCS 14/15(d)(1), and further prohibits selling, leasing, trading, or otherwise profiting from a person's biometric identifiers or biometric information, 740 ILCS 14/15(c).

20. "Biometric identifiers" include retina and iris scans, voiceprints, scans of hand and fingerprints, and—most importantly here—face geometry. *See* 740 ILCS 14/10. "Biometric information" is separately defined to include any information based on an individual's biometric identifier that is used to identify an individual. *See id.*

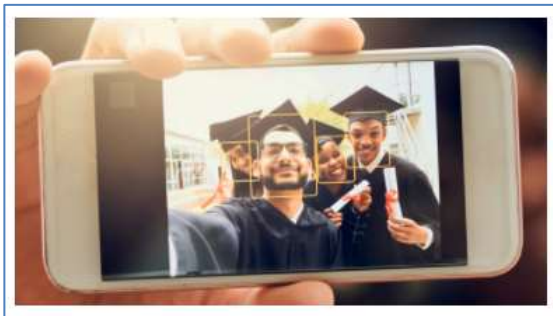
21. The BIPA's narrowly tailored provisions place no absolute bar on the collection, sending, transmitting, or storing of biometric data. For example, the BIPA does not limit what kinds of biometric data may be collected, sent, transmitted, or stored. Nor does the BIPA limit to whom biometric data may be sent or transmitted, or by whom it may be stored. The BIPA simply

mandates that entities wishing to engage in that conduct must make proper disclosures, implement certain reasonable safeguards, and procure a user's consent before collecting biometric data.

III. AWS Violates the BIPA.

22. Despite the BIPA being in force for over a decade, AWS operates a major biometric-based facial recognition platform in violation of the BIPA's simple requirements.

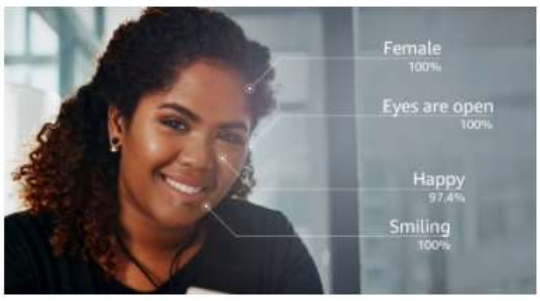
23. Amazon Rekognition is a cloud-based service that, according to Amazon, makes it easy for its customers—from startups to leading corporations—to add image and video analysis, all performed by AWS through its Rekognition platform, to their applications, products, and services. To use its service, an AWS customer just needs to provide AWS an image or video, and then Rekognition can identify objects, people, text, scenes, and activities within the images or video. Amazon even boasts that Rekognition provides facial analysis, face comparison, and face search capabilities, including detecting, analyzing, and comparing faces for a wide variety of use cases, including user verification, cataloging, and people counting. *See* Figures 1 and 2 below, showing screenshots from Amazon's AWS marketing materials.



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.**)

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.