

1 and proof of Plaintiff's current ownership of Amazon stock. The Company received the letter
2 on September 23, 2020.¹

3 1.3 In the Inspection Demand, Plaintiff explained that she wishes to investigate
4 potential wrongdoing occurring at the Company, including potential breaches of fiduciary duty.
5 Plaintiff has legitimate concerns as to whether Amazon violated the Illinois Biometric
6 Information Privacy Act ("BIPA") and whether the Company was engaging in antitrust
7 violations.

8 1.4 The Inspection Demand provided ample evidence of such possible wrongdoing
9 and mismanagement at Amazon. Concerning BIPA, the Inspection Demand explained that
10 Amazon had been developing facial recognition software for years and purchased International
11 Business Machines Corporation's ("IBM") "Diversity in Faces" dataset in 2019 to improve this
12 software. In developing this facial recognition software, Amazon collected, stored, and used
13 individuals' biometric identifiers without ever informing those before, a direct violation of
14 BIPA.

15 1.5 Regarding Amazon's anticompetitive violations, the Inspection Demand again
16 contained detailed information how the Company uses third-party seller data it has access to as
17 an effective middleman to develop its own competing suite of products. The Company then
18 undercuts the third-party on price. Amazon's anticompetitive actions have led to investigations
19 by, at a minimum: (i) the U.S. Congress; (ii) the European Union; (iii) the State of California;
20 and (iv) the State of Washington. Accordingly, Plaintiff has ample reason to suspect
21 wrongdoing at Amazon, more than satisfying the credible basis standard necessary to justify the
22 inspection.

23 ¹ True and correct copies of the Inspection Demand and proof of delivery are attached hereto as Exhibit A and B, respectively.
24

1 and substantial justice. Amazon is headquartered in Washington. Finally, exercising
2 jurisdiction over any nonresident defendant is reasonable under these circumstances.

3 2.2 Venue is proper in this Court because defendant Amazon maintains executive
4 offices in this County, a substantial portion of the transactions and wrongs complained of
5 herein, including the defendant's primary participation in the wrongful acts detailed herein
6 occurred in this County, and defendant has received substantial compensation in this County by
7 doing business here and engaging in numerous activities that had an effect in this County.

8 **III. THE PARTIES**

9 3.1 Plaintiff Michele Rosati is an owner of Amazon's common stock.

10 3.2 Defendant Amazon is a Delaware corporation with principal executive offices
11 located at 410 Terry Avenue North, Seattle, Washington.

12 **IV. THE COMPANY'S UNAUTHORIZED COLLECTION OF INDIVIDUALS'** 13 **INFORMATION VIOLATES THE LAW**

14 **Biometrics and Facial Recognition Technology**

15 4.1 Biometrics is the technical term for measurements used to identify people's
16 unique physical characteristics. Examples of biometric identifiers include an individual's DNA,
17 fingerprints, irises or retinas, voiceprints, and facial geometry. The uniqueness and potential
18 permanence of biometric identifiers present an advantage for businesses to accurately identify
19 and distinguish individuals. Businesses presently use biometrics in a wide variety of
20 applications, including data collection.

21 4.2 One technological application of biometrics is facial recognition software.
22 Facial recognition software uses biometrics to map facial features from a photograph or video.
23 In particular, the software uses an algorithm that calculates a unique digital representation of the
24 face based on the geometric relationship of a person's facial features (such as the distance

1 between their eyes, ears, and nose), creating a face signature or map. The software then
2 compares the information with a database of known faces to find a match.

3 4.3 Facial recognition technology has seen steady improvement over the past decade.
4 Lower costs and increased accuracy have allowed companies such as Amazon to deploy
5 increasingly sophisticated facial recognition software in their applications. However, this
6 increased sophistication has raised serious privacy concerns. Biometrics present potential
7 privacy threats to the individual if compromised, such as a heightened risk for identity theft.
8 During a U.S. Senate hearing in 2012 on the use of facial recognition technology, Senator Al
9 Franken noted that "[o]nce someone has your faceprint, they can get your name, they can find
10 your social networking account, and they can find and track you in the street, in the stores that
11 you visit, the Government buildings you enter, and the photos your friends post online." He
12 added, "facial recognition technology can allow others to access all of that information from a
13 distance, without your knowledge and in about as much time as it takes to snap a photo."
14 Faceprints can even be used to identify protesters at political rallies and "target them for
15 selective jailing and prosecution, stifling their First Amendment rights."

16 4.4 The U.S. Federal Trade Commission ("FTC") has also noted the public's
17 concerns over privacy in social networks that "databases of photos or biometric data may be
18 susceptible to breaches and hacking." The FTC urged companies using facial recognition
19 technology to ask for consent *before* collecting biometric information from a photo. In its best
20 practices guidelines, the FTC addressed social networks in particular, stating, "before using
21 facial recognition to identify an individual it could not otherwise identify, the company should
22 obtain the affirmative express consent of the individual in the image."

23 ///

24

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.