EXHIBIT A

Primary Contact:	Ms. Lynn Radliff Amazon.Com, Inc. 440 Terry Ave N Seattle, WA 98109-5210
Electronic copy provided to:	Rochelle Lewis Scotty Bauder Rebecca Hartley Kimberly Thomas Lizette Fernandez Theresa Nixon Karen Curtis Lynn Foley-Jefferson Joell Parks Gianmarco Vairo Christine Schram Stephen Swisher Sara Rawson Michelle King Annamaria Taskai Maria Catana Eugide Matondo Jesse Jensen

Entity:	Amazon Web Services, Inc. Entity ID Number 2684737
Entity Served:	Amazon Web Services, Inc., A Delaware Corporation
Title of Action:	Asia Hryniewicki vs. Amazon Web Services, Inc.
Document(s) Type:	Summons/Complaint
Nature of Action:	Class Action
Court/Agency:	Lake County Circuit Court, IL
Case/Reference No:	19CH00001155
Jurisdiction Served:	Delaware
Date Served on CSC:	10/22/2019
Answer or Appearance Due:	30 Days
Originally Served On:	CSC
How Served:	Personal Service
Sender Information:	Jad Sheikali 312-893-7002

Information contained on this transmittal form is for record keeping, notification and forwarding the attached document(s). It does not constitute a legal opinion. The recipient is responsible for interpreting the documents and taking appropriate action.

To avoid potential delay, please do not send your response to CSC

251 Little Falls Drive, Wilmington, Delaware 19808-1674   (888) 690-2882 | sop@cscglobal.com

IN THE CIRCUIT COURT OF THE
NINETEENTH JUDICIAL CIRCUIT
LAKE COUNTY, ILLINOIS

ASIA HRYNIEWICKI, individually and on behalf of similarly situated individuals,)))	
Plaintiff,))	No. 19CH00001155
)	
v.)	Hon.
)	
AMAZON WEB SERVICES, INC., a) Delaware corporation.))	**Jury Trial Demanded**
Defendant.)	

CLASS ACTION COMPLAINT AND JURY DEMAND

Plaintiff Asia Hryniewicki ("Plaintiff"), individually and on behalf of other similarly situated individuals, brings this Class Action Complaint against Defendant Amazon Web Services, Inc. ("Defendant") for its violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA"). Plaintiff alleges as follows based on personal knowledge as to her own acts and experiences, and as to all other matters, upon information and belief, including an investigation conducted by her attorneys.

INTRODUCTION

1. BIPA defines a "biometric identifier" as any personal feature that is unique to an individual, including fingerprints and hand geometry. "Biometric information" is any information based on a biometric identifier, regardless of how it is converted or stored. 740 ILCS 14/10. Collectively, biometric identifiers and biometric information are known as "biometrics."

2. Defendant is a leading cloud provider in the United States, offering its customers the ability to store their data, access their data remotely, and create back-up copies of their data.

3.   Defendant stores a myriad of types of data on behalf of a wide range of customers spanning virtually every industry sector.

4.   Notably, Defendant also offers cloud storage services for businesses that handle biometric identifiers and biometric information. For example, some of Defendant's customers are commercial businesses that require their employees to provide their biometrics, e.g. fingerprints, to check in and out of their shifts at work. In such a scenario, Defendant stores data and information that is generated as a result of the capture, collection, and processing of biometric identifiers. This information is considered "biometric information" subject to regulation under BIPA.

5.   Indeed, BIPA not only regulates the conduct of entities that capture and collect biometric identifiers, such as many of Defendant's commercial customers, but also of entities that store data and information derived from those biometric identifiers, like Defendant.

6.   BIPA provides, *inter alia*, that private entities, such as Defendant, may not store an individual's biometric identifiers, such as fingerprints and hand scans, or any biometric information, including any data regardless of the manner from which it was converted, or is converted or stored, unless they first:

   a.   inform that person in writing that biometric identifiers or biometric information will be stored;

   b.   inform that person in writing of the specific purpose and the length of term for which such biometric identifiers or biometric information is being stored; and

   c.   receive a written release from the person for the storage of their biometric identifiers or biometric information.

740 ILCS 14/15(b)(1)-(3).

7.   BIPA also requires private entities in possession of biometric information to develop a publicly available written policy outlining their biometric data storage and destruction policies. 750 ILCS 14/15(a).

8.   Despite obtaining, storing, and possessing biometric information of thousands of Illinois residents, including Plaintiff's biometrics, on behalf of scores of its customers, Defendant failed to comply with BIPA.

9.   Plaintiff brings this action for statutory damages and other remedies as a result of Defendant's conduct in violating her biometric privacy rights under BIPA.

10.   Compliance with BIPA is straightforward and minimally burdensome. For example, the necessary disclosures may be accomplished through a single sheet of paper or through a prominently featured notice affixed to a biometric-enabled device.

11.   BIPA's requirements bestow a right to privacy in biometrics and a right to make an *informed* decision when electing whether to provide or withhold biometrics.

12.   The deprivation of the statutory rights conferred by BIPA constitutes the actual injuries the Illinois Legislature sought to prevent.

13.   On behalf of herself and the proposed Class and Subclass defined below, Plaintiff seeks an injunction requiring Defendant to comply with BIPA, as well as an award of statutory damages to the Class members and monetary damages to be determined at trial, together with costs and reasonable attorneys' fees.

PARTIES

14.   Defendant Amazon Web Services, Inc., is a Delaware corporation that conducts, and is licensed by the Illinois Secretary of State to conduct, business throughout Illinois, including in Lake County, Illinois.

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.

fastcase
Smarter legal research.