

THE HONORABLE ROBERT S. LASNIK

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

UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

KAELI GARNER, *et al.*,

Plaintiffs,

vs.

AMAZON.COM, INC., *et al.*,

Defendants.

)  
) No. 2:21-cv-00750-RSL  
)

) CONSOLIDATED COMPLAINT-CLASS  
) ACTION  
)

) COMPLAINT FOR VIOLATIONS OF THE  
) CALIFORNIA, FLORIDA, ILLINOIS,  
) MARYLAND, MASSACHUSETTS,  
) MICHIGAN, NEW HAMPSHIRE,  
) PENNSYLVANIA, AND WASHINGTON  
) WIRETAPPING STATUTES; THE  
) WASHINGTON CONSUMER  
) PROTECTION ACT; THE FEDERAL  
) WIRETAP ACT; AND THE STORED  
) COMMUNICATIONS ACT

DEMAND FOR JURY TRIAL

CONSOLIDATED COMPLAINT – CLASS  
ACTION AND DEMAND FOR JURY TRIAL

BYRNES ♦ KELLER ♦ CROMWELL LLP  
38TH FLOOR  
1000 SECOND AVENUE

1 **I. INTRODUCTION**

2 1. This class action lawsuit arises out of Amazon’s practice of using smart-speaker  
3 technology (“Alexa”) to surreptitiously: (a) *intercept*; (b) *eavesdrop*; (c) *record*; (d) *disclose*; or  
4 (e) *use* millions of Americans’ voices and communications, all without their knowledge or consent.  
5 Such conduct blatantly violates Washington’s wiretapping law, which applies nationwide to  
6 Plaintiffs and all members of the Class. The conduct also violates the laws of Florida, New  
7 Hampshire, Massachusetts, California, Maryland, Pennsylvania, Illinois, and Michigan  
8 (collectively, with Washington, “State Wiretapping laws”) – all of which prohibit either the  
9 *interception, eavesdropping, recording, disclosure, or use* of communications without the consent  
10 of all parties to the communications. Defendants here, Amazon.com, Inc. and Amazon.com  
11 Services LLC (collectively, “Amazon” or “Defendants”), are therefore liable as a result of their  
12 egregious violations of the State Wiretapping laws – and are also liable for their violations of the  
13 Washington Consumer Protection Act (“CPA”), the Electronic Communications Privacy Act of  
14 1986 (“Federal Wiretap Act”), and the Stored Communications Act of 1986 (“SCA”). Plaintiffs  
15 Kaeli Garner, Mark Fladd, Stephanie Fladd, Jodi Brust, John Dannelly, Diane McNealy, Michael  
16 McNealy, Lisa Hovasse, Sandra Mirabile, Ricky Babani, Susan Lenehan, Jeffrey Hoyt, Lorlie  
17 Tesoriero, James Robinson, Rosa Comacho, Eric Dlugoss, Julie Dlugoss, Ronald Johnson, Selena  
18 Johnson, Caron Watkins, and Kelly Miller (collectively, “Plaintiffs”) bring this action individually,  
19 and on behalf of a Class of similarly situated individuals (defined below), to redress those  
20 violations of law.

21 2. The State Wiretapping laws are united in the prohibition of Amazon’s conduct  
22 alleged herein.

State	Conduct Prohibited	Statute
Washington	Interception or Recording	Wash. Rev. Code §9.73.030
Florida	Interception or Disclosure or Use; or “Endeavors” to Intercept or Disclose or Use	Fla. Stat. §934.03
New Hampshire	Interception or Disclosure or Use; or “Endeavors” to Intercept or Disclose or Use	N.H. Rev. Stat. §570-A:2
Massachusetts	Interception or Disclosure or Use; or “Attempts” to Intercept or Disclose or Use	Mass. Gen. Laws ch. 272, §99
California	“Tap[ping]” or Reading or Use; or “Attempts” to Read or Use	Cal. Penal Code §631
California	Eavesdropping or Recording	Cal. Penal Code §632
Maryland	Interception or Disclosure or Use; or “Endeavor[s]” to Intercept or Disclose or Use	Md. Code Ann., Cts. & Jud. Proc. §10-402
Pennsylvania	Interception or Disclosure or Use; or “Endeavors” to Intercept or Disclose or Use	18 Pa. Cons. Stat. §5703
Illinois	Overhearing or Transmitting or Recording or Interception or Use or Disclosure	720 Ill. Comp. Stat. §5/14-2
Michigan	Eavesdropping	Mich. Comp. Laws §750.539c

CONSOLIDATED COMPLAINT – CLASS  
ACTION AND DEMAND FOR JURY TRIAL

BYRNES • KELLER • CROMWELL LLP  
38TH FLOOR  
1000 SECOND AVENUE

1           3.       Amazon utilized Alexa technology to *willfully* and *intentionally intercept* and  
2 *eavesdrop* upon the confidential conversations of Plaintiffs and the Class. Amazon then *recorded*  
3 those conversations, permanently storing them in the process. Shockingly, Amazon then *disclosed*  
4 those conversations to third parties, including third-party contractors. Amazon did all this to *use*  
5 those conversations for its own financial benefit, including to provide personalized ads for  
6 consumers. Plaintiffs thereby bring this action on behalf of both registered users and unregistered  
7 persons, who never consented to any interception, recording, disclosure, or use of their  
8 communications.<sup>1</sup>

9           4.       Alexa is an omnipresent feature in Amazon’s products. In addition to Amazon  
10 products utilizing Alexa – such as Echo Dot, Echo Plus, Echo Sub, Echo Show, Echo Input, Echo  
11 Frames eyeglasses, Amazon Fire TV digital media player, Amazon Fire TV sticks, Amazon Alexa  
12 Auto, and Amazon Fire tablets – Amazon has authorized several third-party device manufacturers  
13 to offer products that either come with Alexa capability built-in or that are easily integrated with  
14 Alexa (collectively, “Alexa Devices”).

15           5.       Millions of Americans use Alexa Devices in their homes. People speak to Alexa  
16 about a variety of topics, ranging from prosaic, such as asking Alexa to play music or create a to-  
17 do list, to profoundly private, such as asking Alexa about medical conditions. Most people believe  
18 that when they speak to an Alexa Device, their voice is temporarily processed so that Alexa can  
19 generate a response or carry out the user’s command. No one expects that Alexa is creating  
20 permanent recordings of their voices for Amazon to use for its own commercial gain. Worse,  
21 Amazon records and permanently stores these recordings regardless of whether someone was  
22 intentionally or unintentionally talking to an Alexa Device.

23           6.       The mechanics of Amazon’s illegal conduct work as follows. Alexa Devices are  
24 designed to record and respond to human commands in a simulated voice. While an Alexa Device  
25

26 <sup>1</sup> “Registered users” refers to Alexa Device users who set up the Alexa Device through the use of their Alexa App, as outlined below. “Unregistered persons” refers to people who did not set up the Alexa Device, nor registered it.

1 is “always on,”<sup>2</sup> it is only supposed to respond to commands after an individual says a “wake”  
 2 word, which is usually “Alexa” or “Echo.” Once the Alexa Device recognizes the wake word,  
 3 it then records the ensuing communication. Because Alexa Devices were created to capture voices  
 4 “from anywhere in the room,”<sup>3</sup> they record *anything spoken in its vicinity*. The Alexa Device  
 5 then transmits that recording to Amazon’s servers for interpretation and processing before  
 6 receiving the relevant data back in response. *Amazon then permanently stores a copy of that*  
 7 *recording on its own servers for later use and commercial benefit, warehousing billions of private*  
 8 *conversations in the process.*<sup>4</sup> This practice becomes all the more sinister when one considers the  
 9 widespread proliferation of Alexa Devices, which underscores the magnitude of information Alexa  
 10 is impermissibly capturing and storing.

11 7. Critically, Alexa does not discriminate between registered users and non-registered  
 12 persons for recording purposes. It simply records voices – all of them. This means Alexa routinely  
 13 captures unintentional communications without the knowledge or consent of the individuals  
 14 speaking. This is true regardless of whether someone is talking directly to Alexa, to another  
 15 person, or even to themselves. Anyone within the vicinity of an Alexa Device will have their voice  
 16 recorded.

17 8. In light of Alexa’s eavesdropping capabilities, it is unsurprising that Alexa Devices  
 18 capture a host of extremely personal and private conversations, including conversations about  
 19 one’s family, medical conditions, religious beliefs, political affiliations, confidential professional  
 20 communications, and other personal or private matters. Tellingly, former Amazon executive

21 \_\_\_\_\_  
 22 <sup>2</sup> Smart Home, *Introducing Amazon Echo*, YOUTUBE (Aug. 5, 2016), <https://www.youtube.com/watch?v=CYtb8RRj5r4>.

23 <sup>3</sup> *Id.* (discussing Alexa’s use of “far field technology”).

24 <sup>4</sup> Geoffrey A. Fowler, *Alexa has been eavesdropping on you this whole time*, WASH. POST (May 6, 2019),  
 25 <https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time/>; *see also* Ry Crist, *Amazon and Google are listening to your voice recordings. Here’s what we know about that*, CNET  
 26 (July 13, 2019), <https://www.cnet.com/home/smart-home/amazon-and-google-are-listening-to-your-voice-recordings-heres-what-we-know/> (discussing how Amazon stated that it if you make a purchase via Alexa, it may be used to “provide personalized ads”).

# 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.