

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  
27

**UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE**

NANCY MANYPENNY and KENNETH ENSER,  
individually and on behalf of all others similarly  
situated,

Plaintiffs,

v.

AMAZON.COM, INC., AMAZON.COM  
SERVICES LLC, AMAZON DIGITAL SERVICES  
LLC, and AMAZON TECHNOLOGIES, INC.,

Defendants.

Civil Action No.

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

Plaintiffs Nancy Manypenny and Kenneth Enser (“Plaintiffs”), individually and on behalf of all others similarly situated, hereby allege the following against Defendants Amazon.com, Inc., Amazon.com Services LLC, Amazon Digital Services LLC, and Amazon Technologies, Inc. (collectively, “Defendants” or “Amazon”), based upon *inter alia* the investigation made by their counsel, and based upon information and belief, except for those allegations and experiences specifically pertaining to Plaintiffs which are based upon their personal knowledge.

**NATURE OF THE ACTION**

1. This case arises from the illegal conduct of Defendants Amazon.com, Inc., Amazon.com Services LLC, Amazon Digital Services LLC, and Amazon Technologies, Inc. (collectively “Defendants” or “Amazon”), specifically their sweeping, invidious, surreptitious

1 monitoring, recording, and analyzing of the media American consumers choose to watch on the  
2 television screens they purchased to view in the privacy of their own homes. Defendants conduct  
3 this surveillance through software they install on consumers' TVs to record and analyze every  
4 image, frame, and sound played through the screen. Defendants then take consumers, who spend  
5 hundreds or thousands of dollars on a new TV, and package them as a purchasable good,  
6 unwittingly sold to advertisers interested in knowing exactly what they watch. This practice  
7 violates consumer trust, every traditional notion of personal privacy, and relevant to this lawsuit,  
8 federal and state law.

9         2. When Congress passed the Video Privacy Protection Act in 1988, it sought to  
10 protect against "a new, more subtle and pervasive form of surveillance" resulting from "the trail of  
11 information generated by every transaction that is now recorded and stored in sophisticated  
12 record-keeping systems[.]" S. Rep. No. 100-599, at p. 7 (1988) (statement of Sen. Patrick Leahy).  
13 Moreover, Congress was particularly alarmed about surveillance of Americans' media  
14 consumption, recognizing that:

15                 Books and films are the intellectual vitamins that fuel the growth of individual  
16 thought. The whole process of intellectual growth is one of privacy - of quiet, and  
17 reflection. This intimate process should be protected from the disruptive intrusion of  
a roving eye...These records are a window into our loves, lives, and dislikes.

18 *Id.* (statement of Rep. Al McCandless).

19         3. Unfortunately, the pervasive media surveillance that Congress envisioned in 1988  
20 has not only come to pass but has been amplified beyond anything it could have imagined, due to  
21 technological advances equally unimaginable at the time. Indeed, unbeknownst to American  
22 consumers, many major television (also referred to herein as "TV") manufacturers and operating  
23 system providers now secretly install automatic content recognition software ("ACR") onto TVs,  
24 which then constantly record and transmit data relating to a consumer's use of those TVs.

25         4. With a market capitalization well in excess of \$2 trillion, Amazon is consistently  
26 ranked among the most valuable corporations in the world. Amazon owes its size and success in  
27

1 large part to the breadth of the markets it participates in. Furthermore, Amazon can enter virtually  
2 any consumer market it chooses with aggressive pricing undercutting most if not all competitors.  
3 It can do this because, for Amazon's other businesses, these consumers are the product. Whether  
4 you buy an Amazon tablet, doorbell, smart speaker, fitness tracker, e-reader, HDMI streaming  
5 stick, or television, your device is a window into your behaviors and preferences, and Amazon  
6 gives itself full access to that window.

7 5. This systematic process of productizing consumers is perhaps at its zenith with  
8 Amazon's own Fire TV-branded televisions ("Amazon Fire TVs") and even non-Amazon  
9 televisions manufactured by third parties like Toshiba, Insignia, TCL, and Hisense (the "Third-  
10 Party Fire TVs") that are shipped with Amazon's operating system—Fire TV OS (Amazon Fire  
11 TVs and Third-Party Fire TVs are referred to collectively herein as "Fire TVs").

12 6. Fire TVs do not simply track what apps you use and how long you use them. Every  
13 Fire TV runs Amazon's ACR technology, which tracks the content displayed on the screen and the  
14 audio output through the speakers of the televisions in consumers' living rooms. Through use of  
15 this ACR technology, Amazon knows every video you watch, which parts of those videos you  
16 watch, which parts you pause or rewind, and every word you hear. This surveillance is not just  
17 limited to apps on the Fire TV app store, either. If you connect a game system, DVD or Blu-Ray  
18 Player, a computer, or third-party streaming device to your Fire TV, Amazon is still watching and  
19 recording everything you see and hear (collectively the "Sensitive Information").

20 7. Nor does this information simply sit passively on a server. Amazon's sophisticated  
21 machine learning algorithms review and analyze all of this data to better understand exactly the  
22 kind of content you are watching. And through sophisticated technical analysis of data collected  
23 through the ACR Tool and compiled from other sources, Amazon is able to identify and trace the  
24 Sensitive Information back to specific consumers, even where multiple individuals in a household  
25 use the same Fire TV. Amazon exploits this Sensitive Information by (a) selling highly targeted  
26 advertisements to its corporate advertising clients on the myriad platforms that Amazon owns and  
27

1 operates, and (b) feeding it into Amazon’s massive advertising business, which generated \$68.63  
2 billion in revenue in 2025 alone.<sup>1</sup>

3 8. Plaintiffs and Class Members purchased a Fire TV and had their personal Sensitive  
4 Information tracked by Defendants using the ACR Tool. However, Defendants never obtained  
5 informed consent from Plaintiffs or Class Members to collect their Sensitive Information or to  
6 share it with third parties.

7 9. Moreover, Defendants’ tracking of Fire TV users violated federal and state law,  
8 including the Video Privacy Protection Act (“VPPA”), which was passed specifically to prevent  
9 the disclosure and aggregation of data relating to an individual’s video consumption,<sup>2</sup> the  
10 Electronic Communications Privacy Act (“ECPA”), which was enacted to protect the privacy of  
11 electronic communications from unauthorized interception,<sup>3</sup> state consumer fraud statutes., and  
12 constitutes common law invasion of privacy, breach of implied contract, and unjust enrichment.

13 10. As a result of Defendants’ conduct, Plaintiffs and Class Members have suffered  
14 numerous injuries, including: (i) invasion of privacy; (ii) lack of trust in communicating with  
15 electronics retailers; (iii) emotional distress and heightened concerns related to the release of  
16 Sensitive Information to third parties, (iv) loss of benefit of the bargain; (v) diminution of value of  
17 the Sensitive Information; (vi) statutory damages; and (vii) continued and ongoing risk to their  
18 Sensitive Information.

19 11. Therefore, Plaintiffs seek, on behalf of themselves and a class of similarly situated  
20 persons, to remedy these harms and assert the following statutory and common law claims against  
21 Defendants: Invasion of Privacy; Breach of Implied Contract; Unjust Enrichment; violations of the  
22 Video Privacy Protection Act, 18 U.S.C. § 2710, *et seq.*; and state consumer fraud statutes.

23 \_\_\_\_\_  
24 <sup>1</sup> See Marketplace Pulse, *Amazon Advertising Services Sales (2025)*,  
25 <https://www.marketplacepulse.com/stats/amazon-advertising-services-sales>.

26 <sup>2</sup> S. Rep. No. 100-599, at p. 7 (1988).

27 <sup>3</sup> S. Rep. No. 99-541, at pp. 1-5 (1986).

**JURISDICTION AND VENUE**

12. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of \$5,000,000.00 exclusive of interest and costs, there are over 100 members of the proposed class, and at least one class member is a citizen of a state different than Defendants.

13. This Court also has federal question jurisdiction under 28 U.S.C. § 1331 because this Complaint alleges questions of federal law under the VPPA (18 U.S.C. § 2710, *et seq.*). This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

14. This Court has general personal jurisdiction over Defendants because Defendants are headquartered in this District and thus have continuous and systematic ties rendering them “at home” here, and because Defendants maintain their principal place of business in this District. This Court has specific personal jurisdiction over Defendants because they contracted with Plaintiffs and other consumers to bring claims *inter alia* related to their Fire TVs in this District, pursuant to the forum selection clause in Amazon’s Conditions of Use, which provides that disputes “will be adjudicated in the state or Federal courts in King County, Washington.”

15. Venue in this judicial district is proper pursuant to 28 U.S.C. § 1391(b)(1) and (b)(2) because Defendants are headquartered in this District, a substantial part of the events or omissions giving rise to the claims occurred in this District, and Amazon’s forum selection clause designates this District as the proper forum.

**PARTIES**

**Plaintiff Nancy Manypenny**

16. Plaintiff Nancy Manypenny is an individual consumer and citizen of the State of Illinois, residing in Elgin, Illinois.

1 17. Plaintiff Manypenny purchased an Amazon Fire TV on or about May 28, 2024,  
2 from Amazon’s website. She has used her Amazon Fire TV from the purchase date up through the  
3 present to watch television programs and stream video content, including Amazon Prime Video,  
4 Netflix, HBO Max, YouTube, WNBA, TLC Go, Pluto, and Sling TV. Plaintiff Manypenny does  
5 not use any external streaming devices and uses both pre-installed and downloaded applications  
6 directly on the Fire TV.

7 18. Upon inspection, Plaintiff Manypenny verified that the “Device Usage Data,”  
8 “Collect App Usage Data,” and “Interest-Based Ads” settings on her Fire TV were enabled by  
9 default. Upon discovering these settings, she turned them off.

10 19. Unbeknownst to Plaintiff Manypenny, the ACR Tool surreptitiously intercepted  
11 and disclosed the Sensitive Information that was communicated to and from Plaintiff Manypenny  
12 as she used her Amazon Fire TV, including every frame shown and word spoken in the programs  
13 she watched, applications she used, and other information displayed on her television screen  
14 through the normal course of use.

15 20. Plaintiff Manypenny never authorized Defendants to collect, store, analyze,  
16 monetize, and/or disclose her personally identifiable Sensitive Information.

17 **Plaintiff Kenneth Enser**

18 21. Plaintiff Kenneth Enser is an individual consumer and citizen of the State of New  
19 York, residing in Springville, New York.

20 22. Plaintiff Enser purchased a Toshiba 55C350LU television running Fire OS version  
21 7.7.0.8 on or about October 9, 2024, from Best Buy. The Toshiba 55C350LU is a Third-Party Fire  
22 TV—a non-Amazon television that ships with and runs Amazon’s Fire TV operating system.  
23 Plaintiff Enser has used his Toshiba Fire TV from the purchase date up through the present to  
24 watch television programs and stream video content, including Pluto, Paramount+, Tubi,  
25 YouTube, TLC, Fire TV Channels, Amazon Video, and Amazon Music.

1 23. Unbeknownst to Plaintiff Enser, the ACR Tool surreptitiously intercepted and  
2 disclosed the Sensitive Information that was communicated to and from Plaintiff Enser as he used  
3 his Toshiba Fire TV, including every frame shown and word spoken in the programs he watched,  
4 applications he used, and other information displayed on his television screen through the normal  
5 course of use.

6 24. Plaintiff Enser never authorized Defendants to collect, store, analyze, monetize,  
7 and/or disclose his personally identifiable Sensitive Information.

8 **Defendant Amazon.com, Inc.**

9 25. Defendant Amazon.com, Inc. is a for-profit corporation incorporated in the State of  
10 Delaware, with its principal place of business and headquarters located at 410 Terry Avenue  
11 North, Seattle, Washington 98109, in this District. Amazon.com, Inc. is the parent entity of the  
12 Amazon corporate family and develops and operates the Fire TV operating system, Fire TV  
13 hardware products, and the Amazon advertising platform by itself and through its subsidiaries.

14 **Defendant Amazon.com Services LLC**

15 26. Defendant Amazon.com Services LLC is a limited liability company organized  
16 under the laws of the State of Delaware, with its principal place of business located in Seattle,  
17 Washington, in this District. Amazon.com Services LLC operates as the operational backbone for  
18 Amazon's e-commerce, logistics, fulfillment, and customer service operations, and is involved in  
19 the distribution and sale of Fire TV products.

20 **Defendant Amazon Digital Services LLC**

21 27. Defendant Amazon Digital Services LLC is a limited liability company organized  
22 under the laws of the State of Delaware, with its principal place of business located in Seattle,  
23 Washington, in this District. Amazon Digital Services LLC operates Amazon's digital content and  
24 streaming services, including Amazon Prime Video, Freevee, Amazon Music, and Fire TV  
25 Channels—the very on-demand video platforms through which Defendants deliver prerecorded  
26

1 video content to Fire TV users and through which the ACR Tool collects and transmits Plaintiffs’  
2 and Class Members’ Sensitive Information.

3 **Defendant Amazon Technologies, Inc.**

4 28. Defendant Amazon Technologies, Inc. is a for-profit corporation incorporated in  
5 the State of Nevada, with its registered office in Carson City, Nevada. Amazon Technologies,  
6 Inc. holds the patents and intellectual property underlying Amazon’s technologies, including  
7 patents related to the ACR Tool and other data collection, machine learning, and advertising  
8 technologies deployed on Fire TVs.

9 **FACTUAL BACKGROUND**

10 **A. AMAZON’S SURVEILLANCE OF ITS FIRE TV CUSTOMERS**

11 *i. Amazon’s Fire TV Business*

12 29. Amazon launched the first Fire TV device in April 2014 as a streaming media  
13 player. Since then, Amazon has expanded its Fire TV product line to include Fire TV Sticks, Fire  
14 TV Cubes, and—critically to this lawsuit—complete television sets running the Fire TV operating  
15 system.

16 30. Amazon’s Fire TV OS is built on the Android Open Source Project (“AOSP”) and  
17 serves as the software platform for all Fire TV products. Fire TV OS powers not only Amazon-  
18 branded Fire TVs but also televisions manufactured by third parties including Toshiba, Insignia,  
19 TCL, and Hisense, among others.

20 31. As of 2024, Amazon has sold over 250 million Fire TV devices globally, with over  
21 200 million active devices worldwide.<sup>4</sup> In the North American TV operating system market, Fire  
22 TV OS holds approximately 13% market share as of Q1 2025.<sup>5</sup>

23  
24  
25 <sup>4</sup> See Coolest Gadgets, *Streaming Devices Statistics* (2024), <https://coolest-gadgets.com/streaming-devices-statistics/>.

26  
27 <sup>5</sup> See *id.*

1 32. Almost all consumer TVs today are Smart TVs. Consumers have become  
2 accustomed to purchasing TVs with the apps they want installed or available for easy download  
3 directly on the TV's operating system. They do not expect that, in return, the TV manufacturer  
4 will spy on them, monitoring, recording, analyzing, and exploiting for profit everything they  
5 watch.

6 33. Unfortunately, the allure of productizing consumers to pad companies' bottom lines  
7 is sweeping over the industry. More and more Smart TV OEMs are surreptitiously shipping with  
8 ACR surveillance technology embedded in their OS. As one commentator explains:

9 [T]he entry of Chinese manufacturers including Hisense and TCL into the TV  
10 business in the 2000s [led] to unprecedented price competition [for Sony and other  
11 major TV retailers]. As the retail price of TVs fell, the margins of TV manufacturers  
12 became wafer-thin. Average margins in TV hardware are now less than 1%, whereas  
13 margins in connected TV advertising are 50% or more. Faced with these shrinking  
14 hardware margins, manufacturers have increasingly turned to services – advertising,  
15 content sales, and data brokerage – to improve their bottom lines.<sup>6</sup>

14 34. Amazon has readily embraced this trend, enthusiastically moving to increase the  
15 profitability of its Fire TV business through the collection and monetization of customer data.  
16 Amazon's advertising business has become one of the fastest-growing and most profitable  
17 segments of the entire corporation. In 2024, Amazon generated \$56 billion in advertising revenue,  
18 growing to \$68.63 billion in 2025—a 22% year-over-year increase.<sup>7</sup> Today, Amazon is the third-  
19 largest digital advertising company in the world, behind only Google and Meta.

20 35. Fire TV is a strategic platform within this advertising empire. Amazon requires that  
21 third-party apps on Fire TV with over 50,000 hours of monthly usage in the United States  
22 integrate with Amazon Publisher Services and provide Amazon 30% of their in-country  
23

---

24 <sup>6</sup> Ramon Lobato, *Automated content recognition (ACR), smart TVs, and ad-tech infrastructure*,  
25 31(6) *Convergence: The International Journal of Research into New Media Technologies* (July 15,  
26 2025), at 1806, <https://journals.sagepub.com/doi/10.1177/13548565251327885>.

27 <sup>7</sup> See Marketplace Pulse, *Amazon Advertising Services Sales (2025)*, *infra*.

1 advertising impressions.<sup>8</sup> Amazon features banner advertisements on the Fire TV home screen and  
2 sells context-relevant search ads when consumers browse the Fire TV catalog.

3 36. Amazon’s unique competitive advantage in the advertising market is its ability to  
4 combine television viewing data collected through Fire TV with first-party e-commerce shopping  
5 data from Amazon.com. This allows Amazon to offer advertisers behavioral targeting, in-market  
6 audience targeting, and life event targeting that no other advertising platform can match—all  
7 powered by the viewing data secretly collected from Fire TV users.

8 *ii. Fire TV OEM Partners: Third-Party Fire TVs*

9 37. In addition to selling its own Amazon-branded Fire TV televisions, Amazon  
10 licenses its Fire TV operating system to third-party television manufacturers (“OEMs”). These  
11 Third-Party Fire TVs are manufactured by companies including Toshiba, Insignia, TCL, and  
12 Hisense, but run Amazon’s Fire TV OS as their native operating system.<sup>9</sup>

13 38. Toshiba—whose television brand has been licensed to Hisense since 2017—  
14 manufactures a range of Fire TV Edition televisions running Fire TV OS, including the Toshiba  
15 55C350LU model purchased by Plaintiff Enser.<sup>10</sup>

16 39. Insignia, Best Buy’s house brand, is manufactured by Hisense and TCL in Chinese  
17 factories and exclusively uses Fire TV OS.<sup>11</sup>

18 40. All Third-Party Fire TVs run the same Fire TV OS developed and controlled by  
19 Amazon. Amazon controls the ACR technology, data collection settings, privacy policies, and  
20 advertising infrastructure on all Fire TVs, regardless of the hardware manufacturer. The ACR Tool

---

21  
22 <sup>8</sup> See Amazon Developer, *Fire TV Advertising Policy*, <https://developer.amazon.com/docs/policy-center/amazon-appstore-advertising.html>.

23 <sup>9</sup> See BGR, *Amazon Fire TVs: Here's Who Makes Them And Where They're Manufactured*,  
24 <https://www.bgr.com/1994657/who-makes-where-manufactured-amazon-fire-tvs/>.

25 <sup>10</sup> See Tech Junctions, *Who Makes Insignia TVs? (Best Buy's Secret)* (2024),  
26 <https://techjunctions.com/who-makes-insignia-tvs/>.

27 <sup>11</sup> *Id.*

1 (and indeed the entire “software stack”) operates identically on Amazon Fire TVs and Third-Party  
2 Fire TVs.

3 41. Thus, consumers who purchase Third-Party Fire TVs are subjected to the same  
4 ACR surveillance and data collection practices as consumers who purchase Amazon-branded Fire  
5 TVs. Amazon collects, processes, and monetizes the Sensitive Information of all Fire TV users  
6 through the same technical infrastructure and for the same commercial purposes.

7 *iii. Amazon’s Use of the ACR Tool to Surveil Plaintiffs and Class Members*

8 42. Amazon’s ACR technology uses digital fingerprinting methodology. The ACR  
9 Tool creates a digital fingerprint of content from encoded audio or pixel samples captured from  
10 the Fire TV screen, then matches that fingerprint with a database of known movies, TV shows,  
11 advertisements, and other content. When the fingerprint matches, Amazon’s ACR servers can  
12 determine exactly what piece of content is being watched, when, and for how long.<sup>12</sup>

13 43. The ACR Tool installed on Fire TVs operates by recording the image and audio  
14 played by the Fire TV screen continuously whenever the TV is in-use. Then, this output is  
15 analyzed by deep learning software programs to identify whatever visual elements are present on  
16 the screen, such as a specific face, product, brand name, or object. The resulting “video footprint”  
17 created by the ACR Tool is then compared to a content database to determine the specific program  
18 being viewed by the Fire TV user.<sup>13</sup>

19 44. However, the ACR Tool tracks far more than simply the television programs  
20 enjoyed by its customers. Rather, ACR takes in everything on your screen, not just TV shows.  
21 ACR is capturing anything that appears on your screen, including YouTube videos, personal  
22

---

23 <sup>12</sup> While Amazon uses its own proprietary ACR software developed internally, it does not differ  
24 materially in function from well-documented third-party software like the ACR developed and  
25 offered by Samba TV. *See Understanding Video-based Automatic Content Recognition*, Samba  
26 TV at 6, white paper available at <https://www.samba.tv/resources/understanding-video-based-automatic-content-recognition-acr>.

27 <sup>13</sup> *See id.* at 8.

1 photos, security or doorbell camera streams, and video or photos you send via Apple AirPlay or  
2 Google Cast. ACR can even monitor, record, and analyze content from other devices connected to  
3 your TV by HDMI, including personal laptops, video game consoles, and Blu-ray players.<sup>14</sup>

4 45. This creates a detailed log of a household’s media consumption—from what  
5 content was watched, when, and for how long—across all inputs and apps.

6 46. Furthermore, because ACR, metadata, and identifiers combine, the collected data  
7 becomes more than just “what show a consumer watched.” ACR captures or infers highly personal  
8 attributes pertaining to consumers’ race, sex, or religious and political beliefs, all of which fall  
9 under sensitive personal data categories under virtually every privacy regime both nationally and  
10 internationally.

11 47. Amazon builds profiles on consumers based on what genre, when, how often, and  
12 what content consumers see. These yield “household-level content viewership” that is used for  
13 advertising. Amazon’s consumer profiles include cross-device or cross-screen linkage, meaning  
14 that data collected from Fire TVs is correlated with other online activity—including Amazon.com  
15 shopping behavior—and smart devices to facilitate cross-device ad targeting and tracking.

16 48. Amazon ACR data collection, when combined with identifiers, metadata, and  
17 network information, becomes a powerful tool for profiling, targeting, and behavioral tracking,  
18 often without informed consent. Amazon’s profiles on consumers include intimate details like  
19 political leanings, sexual orientation, health interests, marital status, family composition and age,  
20 and religion.

21 49. Fire TVs are not a passive mode of entertainment, but a relentless surveillance  
22 unless a consumer learns of the surreptitious ACR surveillance software and deactivates it.

23  
24  
25 <sup>14</sup> Rachel Cericola, Jon Chase and Lee Neikirk, *Yes, Your TV Is Probably Spying on You. Your*  
26 *Fridge, Too. Here’s What They Know*, New York Times (June 25, 2025),  
27 <https://www.nytimes.com/wirecutter/reviews/advice-smart-devices-data-tracking/>.

1           50. As the ACR Tool collects and analyzes all of the information displayed on the  
2 user's Fire TV screen at all times, some of the information captured necessarily includes highly  
3 sensitive, personally identifiable information. For example, when a user logs into a streaming app  
4 or video game platform (e.g., Netflix, Hulu, PlayStation Plus), the ACR Tool may capture the e-  
5 mail address associated with the user's account. If the user accesses an account information page  
6 in a streaming application, the ACR Tool may capture the user's account information, including  
7 the user's full name, address, and billing information. Moreover, as Fire TVs can be used as a  
8 computer monitor, the ACR Tool could even capture extensive, highly sensitive information  
9 accessed by the user online, such as information from medical provider online portals, banking  
10 provider financial portals, and communicated through social media and e-mail messages.

11           51. Through this highly invasive data collection, the ACR Tool amasses a wealth of  
12 intimate knowledge about Fire TV owners, allowing Amazon to target consumers based on highly  
13 sensitive attributes such as religion, political affiliation, and ethnicity.

14           52. Further, as if this mass surveillance were not bad enough already, Amazon's  
15 misuse of its customers' Sensitive Information is not limited to merely its own advertising  
16 operations. Amazon feeds ACR-derived data into its massive advertising platform, which makes  
17 this data available to advertisers who purchase targeted advertising to productized consumers  
18 through Amazon's demand-side platform ("DSP"). While Amazon has stated that it "never sells or  
19 rents customers' personal data," the fact is that Amazon sells direct, targeted access to customers  
20 based on their personal data. Thus, Fire TV users' Sensitive Information is exploited for third-  
21 party commercial gain without the users' knowledge or consent.

22 **B. PLAINTIFFS AND CLASS MEMBERS DID NOT CONSENT TO AMAZON'S**  
23 **COLLECTION AND MONETIZATION OF THEIR SENSITIVE INFORMATION**  
24 **THROUGH THE ACR TOOL**

25 *i. Plaintiffs' and Class Members' Reasonable Expectation of Privacy*

26           53. At all times when Plaintiffs' and Class Members' Sensitive Information was  
27 surreptitiously monitored and recorded by Amazon through the ACR Tool, they each had a

1 reasonable expectation that the content they viewed in the (supposed) privacy of their own homes  
2 would remain confidential and that Amazon would not monitor, record, analyze, or exploit the  
3 Sensitive Information with third parties for commercial purposes.

4 54. Privacy polls and studies show that the overwhelming majority of Americans  
5 consider obtaining an individual’s affirmative informed consent before a company collects and  
6 shares that individual’s data to be one of the most important privacy rights.

7 55. For example, studies have shown that 85-percent of Americans believe that internet  
8 companies and websites should be required to obtain consent before selling or sharing consumer  
9 data.<sup>15</sup>

10 56. Personal data privacy and obtaining consent to share Sensitive Information are  
11 material to Plaintiffs and Class Members.

12 *ii. Plaintiffs Did Not (and Could Not) Consent to Amazon’s Surveillance Practices*

13 57. Amazon’s Fire TV user interface (“UI”) reveals a surveillance-by-default design  
14 philosophy that is intended to manipulate consumer consent to align with its business interests.  
15 This scheme is illustrated in the following ways.

16 58. When setting up a new Fire TV, the first screen prompts the user to select their  
17 language. After selecting a language, the next screen displays a prominent ‘Continue’ button with  
18 fine print at the bottom of the screen stating “By clicking ‘Continue’ or ‘Store Use’, you agree to  
19 Amazon’s Conditions of Use at [www.amazon.com/conditionsofuse](http://www.amazon.com/conditionsofuse) and all the terms found at  
20 [www.amazon.com/devicesupport](http://www.amazon.com/devicesupport) or here.” This fine print also notes that “Amazon processes and  
21 retains audio, interactions, viewing, and other data in the cloud to provide and improve our  
22 services.” Nowhere does this fine print give notice of the scope of surveillance by Amazon’s  
23  
24

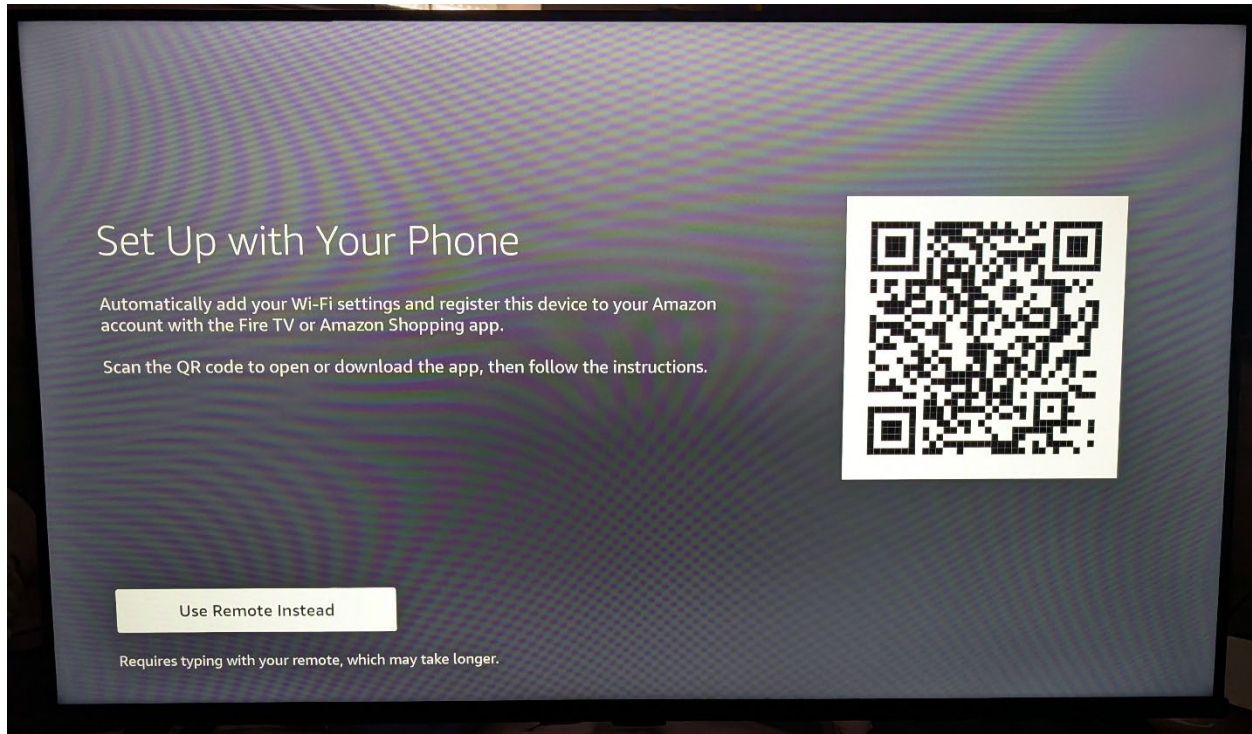
---

25 <sup>15</sup> See Darrel M. West, *Brookings survey finds three-quarters of online users rarely read business*  
26 *terms of service*, Brookings (May, 2019), <https://www.brookings.edu/articles/brookings-survey-finds-three-quarters-of-online-users-rarely-read-business-terms-of-service/>.

1 ACR software nor does it give notice that any of that surveillance will be shared with third parties  
2 and/or used to target consumers with advertising:



14 59. Once the purchaser clicks continue, they are prompted to set up their Fire TV  
15 account on their phones and, as an alternative, may input their account credentials directly onto the  
16 TV to finish setup on the TV:



60. This is the only affirmative action a user takes before the Fire TV setup is complete. The purchaser presses a ‘Continue’ button once, signs into their Amazon account, and the Fire TV is set up. All of its default settings are set with no indication a user can change them or what they are.

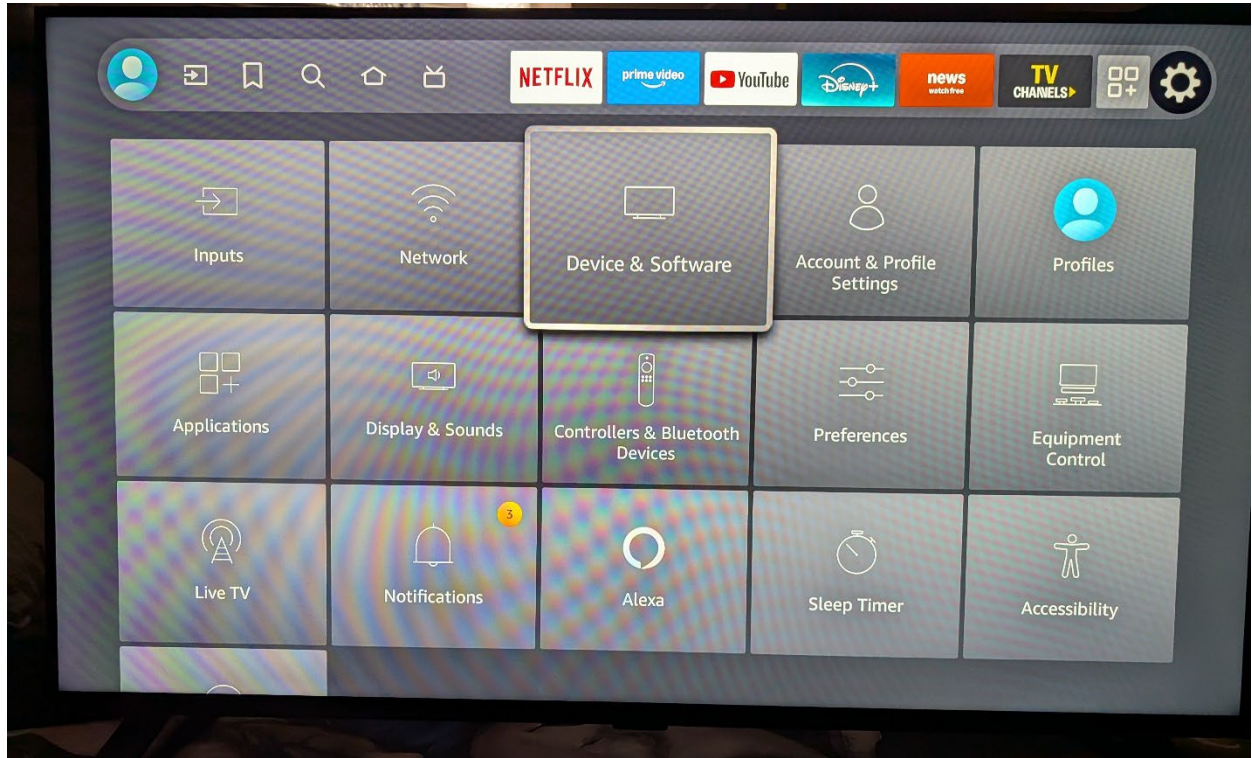
61. Under those default settings, Amazon enables key data collection settings without meaningful disclosure. Specifically, when a consumer sets up a new Fire TV, the following privacy-invasive settings are enabled by default: (a) “Device Usage Data,” which controls the collection of data about how consumers navigate the home screen, select device settings, and open and close applications; (b) “Collect App Usage Data,” which controls collection of data about third-party app usage including open, close, and duration of use; and (c) “Interest-Based Ads,” which controls interest-based advertising targeting.<sup>16</sup>

---

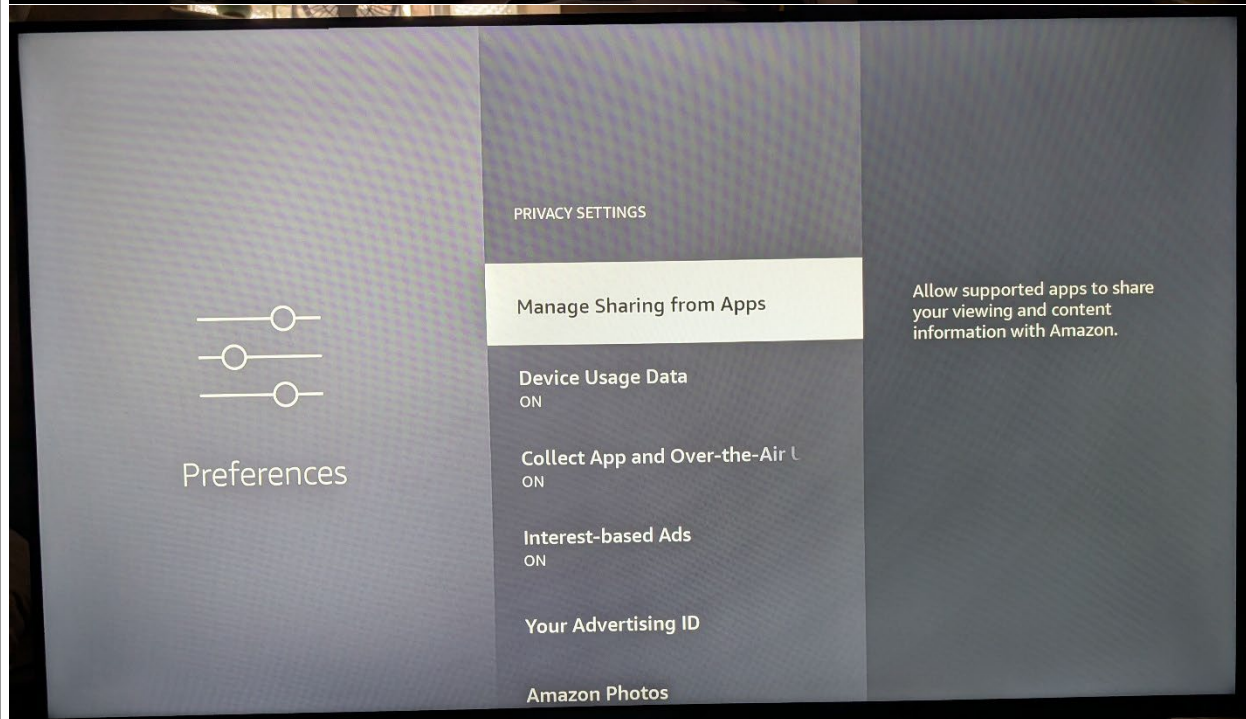
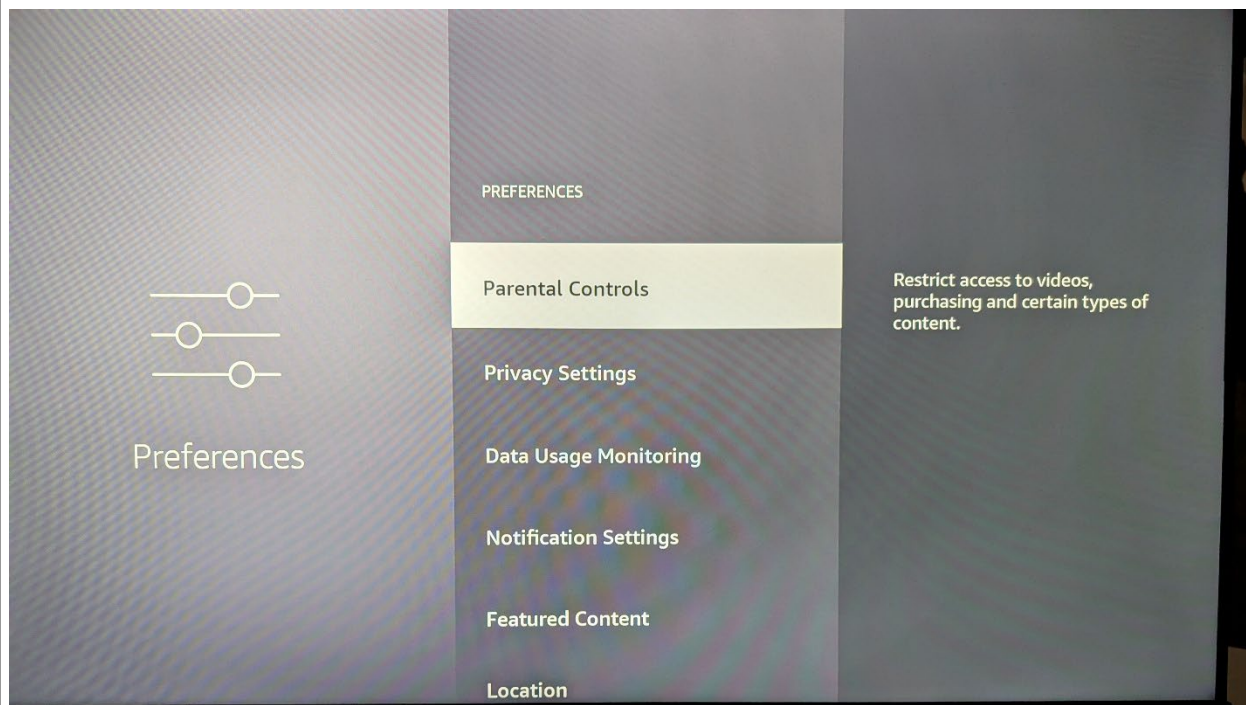
<sup>16</sup> See Amazon, *Fire TV Privacy FAQ*, <https://www.amazon.com/gp/help/customer/display.html?nodeId=GQFYXZH2B2H629WN>.

62. On Fire TV Edition televisions (those with built-in Fire TV OS, including both Amazon Fire TVs and Third-Party Fire TVs), an additional setting—“Collect App and Over-the-Air Usage Data”—is also enabled by default. This setting controls the collection of channel name, program name, and duration of over-the-air television content watched through a connected antenna.<sup>17</sup>

63. Consent is not informed because Amazon buries its privacy controls in a nested, non-intuitive menu hierarchy. To access and modify the ACR-related data collection settings, Fire TV users must navigate through: Settings, then Preferences, then Privacy Settings—a multi-step path that a reasonable consumer would have no reason to explore absent specific knowledge that ACR surveillance is occurring.



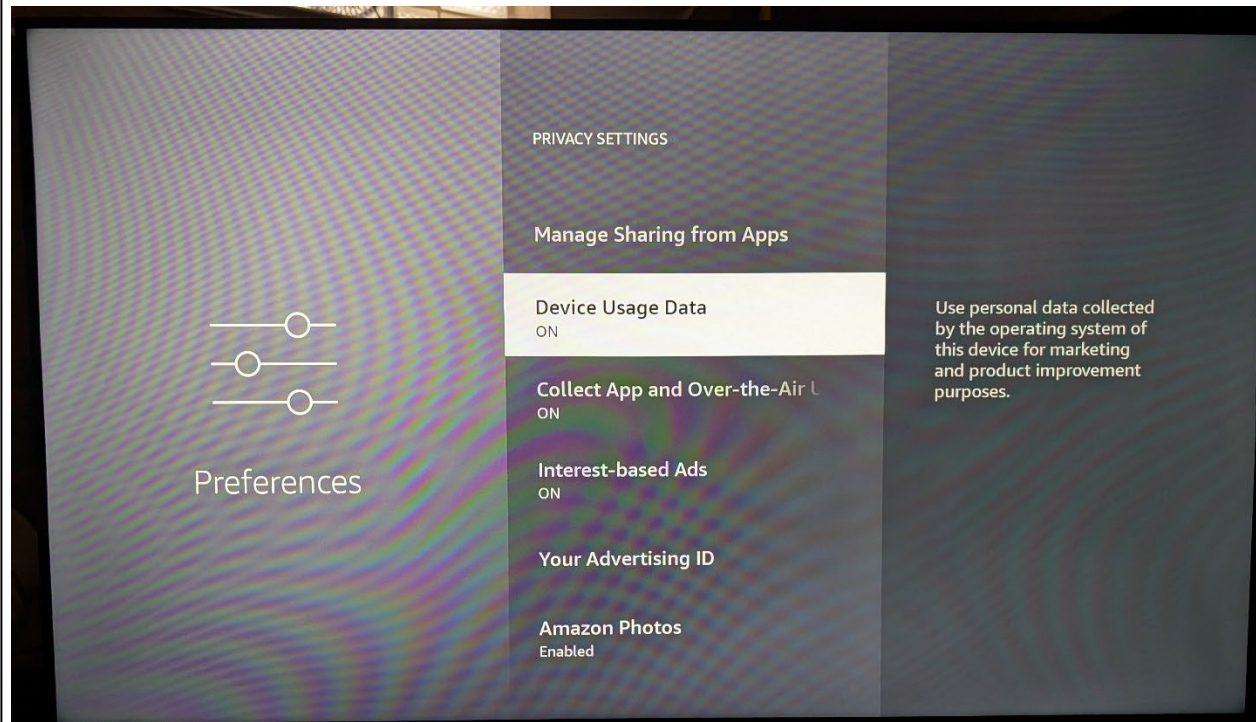
<sup>17</sup> *Id.*



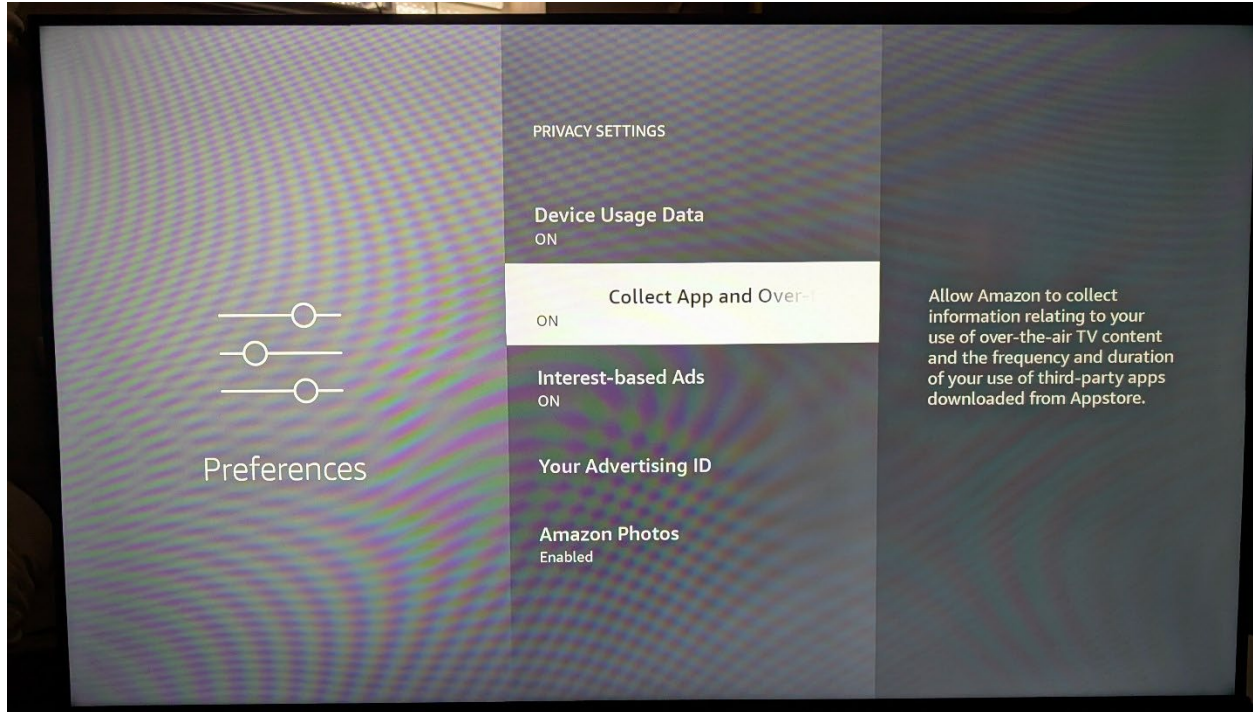
64. Once in that Privacy Settings sub-menu, Amazon’s disclosures regarding its data collection practices are opaque and misleading. Amazon’s privacy disclosures do not clearly explain to consumers that the ACR Tool continuously captures audio and visual data from the Fire TV screen, correlates that data with user-specific identifiers, and feeds it into Amazon’s

1 advertising platform to allow Amazon and other companies to target them. The disclosures use  
 2 vague and euphemistic language—such as “Device Usage Data” and “Collect App and Over-the-  
 3 Air Usage Data”—that does not put consumers on notice that they are consenting to real-time,  
 4 continuous surveillance of everything displayed on their television screen.

5 65. The “Device Usage Data” option simply states: “Use personal data collected by the  
 6 operating system of this device for marketing and product improvement purposes.” It does not  
 7 mention what personal data is shared, or the fact that the personal data includes constant  
 8 monitoring, recording, and analyzing of everything on the purchaser’s screen:



20 66. The “Collect App and Over-the-Air Usage Data” option simply states: “Allow  
 21 Amazon to collect information relating to your use of over-the-air TV content and the frequency  
 22 and duration of your use of third-party apps downloaded from Appstore.” It does not mention  
 23 what personal data is collected or the fact that the personal data includes constant monitoring,  
 24 recording, and analyzing of everything on the purchaser’s screen:



67. Amazon’s opt-out architecture undermines the adequacy of meaningful choice. To fully opt-out of ACR and related data tracking on Fire TVs, consumers must individually disable multiple separate settings—including “Device Usage Data,” “Manage Sharing from Apps,” “Collect App and Over-the-Air Usage Data,” and “Interest-Based Ads”—each of which is located within the buried Privacy Settings menu but must be individually toggled off. In contrast, these settings are all enabled by default during initial setup, requiring no affirmative action by the consumer.

68. The juxtaposition between automatic enrollment by default and the multi-step process required to opt-out is a quintessential example of an “dark pattern,” tricking consumers into sharing more private information than they would have if Defendants had been transparent about their data collection practices and sought to obtain consent as legally required.

69. Amazon’s Privacy Notice accessible on Fire TVs uses opaque and non-intuitive language. Amazon states it “never sells or rents customers’ personal data,” yet simultaneously operates a \$68.63 billion advertising business that is fueled in significant part by the viewing data collected from Fire TV users. This representation is misleading because it obscures the fact that

1 Amazon monetizes consumer data by providing ACR-derived targeting capabilities to advertisers,  
2 which allows companies who pay for access to target specific Fire TV users based on their  
3 personal Sensitive Information.

4 70. Amazon does not clearly explain that it collects, monetizes, and uses a user's  
5 viewing history, along with data reflecting any other actions the customer takes using their Fire  
6 TV. No reasonable consumer could possibly infer from the euphemistic representations in  
7 Amazon's disclosures that the Fire TV captures all video and audio output continuously, correlates  
8 that data with additional user-specific data collected from Amazon's vast ecosystem of other  
9 services, and then provides that data to advertisers in a manner allowing it to be linked to the  
10 consumer's identity. Further, Amazon's disclosures do not put consumers on notice that, not only  
11 is video content that they watch or stream on the Fire TV captured, but if they use a Fire TV's  
12 external input (for example, to connect a video game console or personal computer) then the video  
13 content of the externally connected device will also be captured by the ACR Tool.

14 71. In short, Amazon deliberately designed both the form and content of its ACR  
15 disclosures to obfuscate its invasive surveillance of its customers. The default action of opting into  
16 Amazon's extensive data collection (which requires no action at all, as settings are enabled by  
17 default) versus the convoluted and opaque action of opting out (which requires navigating buried  
18 menus and toggling multiple settings individually) is clearly designed to mislead customers into  
19 sharing Sensitive Information that they would be disinclined to share if Amazon was transparent  
20 about the ACR Tool and its data collection practices.

21 72. Furthermore, even if a particularly sleuthing and tech-savvy consumer manages to  
22 change every one of the privacy settings necessary to disable ACR, Amazon employs further  
23 practices to subvert consumer informed consent. Specifically, when consumers' Fire TV OS  
24 updates, these updates reset many default settings in the OS including these privacy settings.

1 Therefore, a consumer who has affirmatively opted out of every setting necessary to disable ACR  
2 may still be subject to Amazon’s ACR surveillance.<sup>18</sup>

3 **C. AMAZON WAS ENRICHED BY ITS COLLECTION, MONETIZATION, AND**  
4 **UNAUTHORIZED DISCLOSURE OF PLAINTIFFS’ AND CLASS MEMBERS’**  
5 **SENSITIVE INFORMATION**

6 *i. Amazon Derived Significant Benefits from Its Collection and Use of Plaintiffs’ and Class*  
7 *Members’ Sensitive Information*

8 73. As detailed above, the extensive array of data collected by the ACR Tool allows  
9 Amazon to engage in comprehensive, targeted advertising across its entire advertising ecosystem.

10 74. As a direct result of its surreptitious collection, use, and exploitation of Plaintiffs’  
11 and Class Members’ Sensitive Information, Amazon is able to generate tens of billions of dollars  
12 in advertising revenue. In 2025 alone, Amazon’s advertising segment generated \$68.63 billion in  
13 revenue, a 22% increase over the prior year. This advertising revenue represented 9.36% of  
14 Amazon’s total revenue—the highest share ever recorded.<sup>19</sup>

15 75. Fire TV’s contribution to Amazon’s advertising business is strategic and  
16 substantial. Amazon leverages the viewing data collected through Fire TV’s ACR Tool to offer  
17 advertisers uniquely powerful targeting capabilities, including in-market audience targeting, life  
18 event targeting, and behavioral targeting powered by the combination of television viewing data  
19 and Amazon’s e-commerce shopping data.

20 76. Amazon requires that third-party apps on Fire TV with over 50,000 hours of  
21 monthly usage in the United States integrate with Amazon Publisher Services and provide

---

22  
23 <sup>18</sup> [https://www.techtimes.com/articles/315996/20260420/stop-your-smart-tv-tracking-you-simple-](https://www.techtimes.com/articles/315996/20260420/stop-your-smart-tv-tracking-you-simple-settings-that-boost-privacy.htm)  
24 [settings-that-boost-privacy.htm](https://www.techtimes.com/articles/315996/20260420/stop-your-smart-tv-tracking-you-simple-settings-that-boost-privacy.htm) (article informing consumers on ACR surveillance, noting: “Smart  
25 TVs change with firmware updates, and new features or redesigned menus can quietly reintroduce  
26 Tracking, privacy options, ACR tools, and ad targeting defaults. Checking smart TV settings every  
27 few months helps ensure viewing data and advertising controls remain aligned with user  
preferences.”).

<sup>19</sup> See Marketplace Pulse, *Amazon Advertising Services Sales (2025)*, *infra*.

1 Amazon 30% of in-country advertising impressions—effectively extracting a tax on all advertising  
2 revenue flowing through the Fire TV platform, powered by the data collected through the ACR  
3 Tool.

4 *ii. Plaintiffs’ and Class Members’ Data Had Financial Value*

5 77. Moreover, Plaintiffs’ and Class Members’ Sensitive Information had value, and  
6 Defendants’ collection, use, and exploitation of that Sensitive Information harmed Plaintiffs and  
7 the Class.

8 78. According to the financial statements of Facebook, a major data and advertisement  
9 broker, the value derived from user data has continuously risen. Proton, a privacy-centered tech  
10 company estimates that the value of the average American’s data is worth “at least \$700,” with  
11 values to various tech giants ranging between \$217 to \$393.<sup>20</sup>

12 79. The unauthorized collection, use, and exploitation of Plaintiffs’ and Class  
13 Members’ private and Sensitive Information has diminished the value of that information,  
14 resulting in harm to Plaintiffs and Class Members.

15 **D. AMAZON’S USE OF THE ACR TOOL VIOLATES THE VIDEO PRIVACY**  
16 **PROTECTION ACT (“VPPA”)**

17 80. The VPPA was passed in 1988 in response to Congress’s concern that “the trail of  
18 information generated by every transaction that is now recorded and stored in sophisticated  
19 record-keeping systems is a new, more subtle and pervasive form of surveillance.” S.  
20 Rep. No. 100-599, at p. 7 (1988) (statement of Sen. Patrick Leahy).

21 81. Although the VPPA was originally intended to protect the privacy of an  
22 individual’s rental videotape selections, Congress has repeatedly reiterated that the VPPA is  
23 applicable to “‘on-demand’ cable services and Internet streaming services [that] allow consumers  
24

---

25  
26 <sup>20</sup> See *What’s Your Data Really Worth*, Proton (Feb. 8, 2024), <https://proton.me/blog/what-is-your-data-worth>.

1 to watch movies or TV shows on televisions, laptop computers, and cell phones.” S. Rep. 112-258,  
2 at p. 2.<sup>21</sup>

3 82. Under the VPPA, “[a] video tape service provider” is prohibited from “knowingly  
4 disclos[ing], to any person, personally identifiable information concerning any consumer of such  
5 provider” without the consumer’s “informed, written consent... in a form distinct and separate  
6 from any form setting forth other legal or financial obligations of the consumer.” 18 U.S.C.  
7 section 2710(b).

8 83. The VPPA defines a “video tape service provider” as “any person, engaged in the  
9 business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of pre-recorded  
10 video cassette tapes or similar audio-visual materials.” 18 U.S.C. section 2710(a)(4).

11 84. The VPPA additionally defines “personally identifiable information” as  
12 “information which identifies a person as having requested or obtained specific video materials or  
13 services from a video service provider.” 18 U.S.C. section 2710(a)(3).

14 85. Amazon is a video tape service provider within the meaning of the VPPA, as it  
15 provides on-demand access to prerecorded video content through both third-party apps offered  
16 through the Fire TV platform as well as its own content provided to Fire TV users through  
17 Amazon Prime Video, Freevee (formerly IMDb TV), and Fire TV Channels. Indeed, Amazon  
18 operates one of the largest streaming video platforms in the world through Amazon Prime Video.  
19 Accordingly, Defendants’ disclosure of the specific videos viewed by their customers through on-  
20 demand streaming services constitutes a violation of the VPPA. *See, e.g., Fan v. NBA Props. Inc.*,  
21 No. 23-cv-05069-SI, 2024 U.S. Dist. LEXIS 57205, at \*9 (N.D. Cal. Mar. 26, 2024) (“in enacting  
22 the VPPA, ‘Congress[] inten[ded] to cover new technologies for pre-recorded video content’” and  
23 “used ‘similar audio visual materials’ to ensure that VPPA’s protections would retain their force  
24 even as technologies evolve”) (citation omitted).

---

25  
26  
27 <sup>21</sup> S. Rep. 112-258, at p. 2 (2012).

1 **TOLLING AND ESTOPPEL**

2 86. Any applicable statutes of limitation have been tolled by Defendants’ knowing and  
3 active concealment of its installation of the ACR Tool onto Fire TVs.

4 87. The ACR Tool installed on the Fire TVs was and is invisible to the average Fire  
5 TV owner.

6 88. Through no fault or lack of diligence, Plaintiffs and Class Members were deceived  
7 and could not reasonably discover Defendants’ deception and unlawful conduct.

8 89. Plaintiffs were ignorant of the information essential to pursue their claims, without  
9 any fault or lack of diligence on their part.

10 90. Defendants had exclusive knowledge that the ACR Tool was installed on the Fire  
11 TVs and that the data collection settings were enabled by default, and yet failed to clearly disclose  
12 to customers, including Plaintiffs and Class Members, that by using a Fire TV, Plaintiffs’ and  
13 Class Members’ Sensitive Information would be collected, analyzed, and exploited for advertising  
14 purposes.

15 91. Under the circumstances, Defendants were under a duty to disclose the nature,  
16 significance, and consequences of their collection and treatment of their customers’ Sensitive  
17 Information. Accordingly, Defendants are estopped from relying on any statute of limitations.

18 92. Moreover, all applicable statutes of limitation have also been tolled pursuant to the  
19 discovery rule.

20 93. The earliest that Plaintiffs or Class Members, acting with due diligence, could have  
21 reasonably discovered Defendants’ conduct would have been shortly before the filing of this  
22 Complaint.

23 **CLASS ACTION ALLEGATIONS**

24 94. Plaintiffs bring this action on behalf of themselves and all other similarly situated  
25 persons pursuant to Fed. R. Civ. P. 23(a), (b)(1), (b)(2), and (b)(3). Specifically, the following  
26 Classes and Subclasses are defined as:

1 **Nationwide Amazon Fire TV Class:** All persons in the United States who have  
2 owned or used an Amazon-branded Fire TV and whose Sensitive Information was  
3 collected through the ACR Tool without their actual and/or informed consent.

4 **Nationwide Third-Party Fire TV Class:** All persons in the United States who have  
5 owned or used a Third-Party Fire TV, and whose Sensitive Information was collected  
6 through the ACR Tool without their actual and/or informed consent.

7 **Illinois Subclass:** All persons in the state of Illinois who have owned or used a Fire  
8 TV (whether Amazon-branded or third-party-branded) and whose Sensitive  
9 Information was collected through the ACR Tool without their actual and/or  
10 informed consent.

11 **New York Subclass:** All persons in the state of New York who have owned or used  
12 a Fire TV (whether Amazon-branded or third-party-branded) and whose Sensitive  
13 Information was collected through the ACR Tool without their actual and/or  
14 informed consent.

15 **Consumer Fraud Multi-State Subclass:** All persons in the States of California,  
16 Florida, Illinois, Massachusetts, Michigan, Minnesota, Missouri, New Jersey, New  
17 York, and Washington who have owned or used a Fire TV (whether Amazon-  
18 branded or third-party-branded) and whose Sensitive Information was collected  
19 through the ACR Tool without their actual and/or informed consent.<sup>22</sup>

---

20  
21  
22  
23 <sup>22</sup> The States in the Consumer Fraud Multi-State Subclass are limited to those States with similar consumer  
24 fraud laws under the facts of this case: California (Cal. Bus. & Prof. Code § 17200, *et seq.*); Florida (Fla.  
25 Stat. § 501.201, *et seq.*); Illinois (815 Ill. Comp. Stat. 505/1, *et seq.*); Massachusetts (Mass. Gen. Laws Ch.  
26 93A, *et seq.*); Michigan (Mich. Comp. Laws § 445.901, *et seq.*); Minnesota (Minn. Stat. § 325F.67, *et seq.*);  
27 Missouri (Mo. Rev. Stat. § 407.010, *et seq.*); New Jersey (N.J. Stat. § 56:8-1, *et seq.*); New York (N.Y.  
Gen. Bus. Law § 349, *et seq.*); and Washington (Wash. Rev. Code § 19.86.010, *et seq.*). Plaintiffs reserve  
the right to amend and update this definition subject to discovery.

1 95. The Nationwide Amazon Fire TV Class and the Nationwide Third-Party Fire TV  
2 Class are referred to together as the “Nationwide Classes.” The Nationwide Classes and each of  
3 the Subclasses are referred to together as the “Classes” or simply the “Class.”

4 96. Excluded from the Classes are: (a) federal, state, and/or local governments,  
5 including, but not limited to, their departments, agencies, divisions, bureaus, boards, sections,  
6 groups, counsels, and/or subdivisions; (b) any entity in which any Defendant has a controlling  
7 interest, to include, but not limited to, their legal representatives, heirs, and successors; (c) all  
8 persons who are presently in bankruptcy proceedings or who obtained a bankruptcy discharge in  
9 the last three years; and (d) any judicial officer in this lawsuit and/or persons within the third  
10 degree of consanguinity to such judge.

11 97. Plaintiffs reserve the right to amend or otherwise alter the above class definitions  
12 presented to the Court at the appropriate time, or to add or eliminate classes as appropriate, in  
13 response to facts learned through investigation, discovery, and the specific theories of liability, or  
14 otherwise.

15 98. This action is properly maintainable as a class action pursuant to Federal Rule of  
16 Civil Procedure 23 for the reasons set forth below.

17 99. **Numerosity:** The precise number of members of the Classes is unknown to  
18 Plaintiffs, but it is clear the number greatly exceeds the number that would make joinder  
19 practicable. Amazon has sold over 250 million Fire TV devices globally and maintains over 200  
20 million active devices. The number of U.S. Fire TV users whose Sensitive Information was  
21 collected by the ACR Tool numbers in the tens of millions. However, members of the Classes and  
22 their identities may be determined through discovery.

23 100. **Commonality and Predominance:** This action involves common questions of law  
24 or fact, which predominate over any questions affecting individual members of the Classes. All  
25 members of the Classes were exposed to the same data collection practices of Defendants, as  
26 alleged herein. Included within the common questions of law or fact are:

- 1 a. Whether and to what extent Defendants had a duty to protect the Sensitive  
2 Information of Plaintiffs and Class Members;
- 3 b. Whether Defendants had duties not to collect and/or disclose the Sensitive  
4 Information of Plaintiffs and Class Members to unauthorized third parties;
- 5 c. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and  
6 Class Members that their Sensitive Information would be collected and exploited  
7 for advertising purposes;
- 8 d. Whether Defendants violated the law by failing to promptly notify Plaintiffs and  
9 Class Members that their Sensitive Information was being collected and used  
10 without their informed consent;
- 11 e. Whether Defendants adequately addressed and fixed the practices which permitted  
12 the unauthorized collection and use of Plaintiffs' and Class Members' Sensitive  
13 Information;
- 14 f. Whether Defendants violated the Video Privacy Protection Act, as alleged in this  
15 Complaint;
- 16 g. Whether Defendants violated the Illinois Consumer Fraud and Deceptive Business  
17 Practices Act, as alleged in this Complaint;
- 18 h. Whether Defendants violated the New York General Business Law §§ 349-350, as  
19 alleged in this Complaint;
- 20 i. Whether Defendants violated the consumer fraud statutes of the states listed in the  
21 Consumer Fraud Multi-State Class;
- 22 j. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or  
23 nominal damages as a result of Defendants' wrongful conduct; and
- 24 k. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the  
25 imminent and currently ongoing harm faced as a result of the Defendants'  
26 collection and exploitation of their Sensitive Information.

1           **101. Typicality:** Plaintiffs' claims are typical of the claims of other Class Members  
2 because Plaintiffs' Sensitive Information, like that of every other Class Member, was  
3 compromised as a result of Defendants' incorporation and use of the ACR Tool. Plaintiff  
4 Manypenny's claims are typical of the Amazon Fire TV Class, and Plaintiff Enser's claims are  
5 typical of the Third-Party Fire TV Class. Defendants' unlawful, unfair and/or deceptive actions  
6 concern the same business practices described herein irrespective of where they occurred or were  
7 experienced. Plaintiffs and the Class Members sustained similar injuries arising out of Defendants'  
8 conduct. Plaintiffs' and Class Members' claims arise from the same practices and course of  
9 conduct and are based on the same legal theories. Further, there are no defenses available to  
10 Defendants that are unique to Plaintiffs' claims.

11           **102. Adequacy:** Plaintiffs are adequate representatives of the members of the Classes  
12 they seek to represent because their interests do not conflict with the interests of the members of  
13 the Classes they seek to represent. Plaintiffs have retained counsel competent and experienced in  
14 the prosecution of complex class action litigation, including complex questions that arise in  
15 consumer protection and privacy litigation. Plaintiffs and their counsel will prosecute this action  
16 vigorously. The interests of the Classes will be fairly and adequately protected by Plaintiffs and  
17 Plaintiffs' counsel.

18           **103. Superiority:** A class action is superior to any other available means for the fair and  
19 efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered  
20 in the management of this class action. The damages or other financial detriment suffered by  
21 Plaintiffs and the other members of the Classes are relatively small compared to the burden and  
22 expense that would be required to individually litigate their claims against Defendants, so it would  
23 be impracticable for members of the Classes to individually seek redress for Defendants' wrongful  
24 conduct. Even if the members of the Classes could afford individual litigation, the court system  
25 could not. Individualized litigation creates a potential for inconsistent or contradictory judgments  
26 and increases the delay and expense to all parties and the court system.

1           104. By contrast, the class action device presents far fewer management difficulties and  
2 provides the benefits of single adjudication, economy of scale, and comprehensive supervision by  
3 a single court. Given the similar nature of the claims and the absence of material or dispositive  
4 differences in laws upon which the claims are based, the Classes will be easily managed by the  
5 Court and the parties.

6           105. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for  
7 certification because such claims present only particular, common issues, the resolution of which  
8 would advance the disposition of this matter and the parties' interests therein. Such particular  
9 issues include, but are not limited to:

- 10           a. Whether Defendants owed a legal duty to Plaintiffs and the Classes to exercise due  
11 care in collecting, storing, and safeguarding their Sensitive Information and not  
12 disclosing it to unauthorized third parties;
- 13           b. Whether Defendants breached a legal duty to Plaintiffs and Class Members to  
14 exercise due care in collecting, storing, using, and safeguarding their Sensitive  
15 Information;
- 16           c. Whether Defendants failed to comply with applicable laws, regulations, and  
17 industry standards relating to data privacy;
- 18           d. Whether Defendants adequately and accurately informed Plaintiffs and Class  
19 Members that their Sensitive Information would be collected and exploited for  
20 advertising purposes;
- 21           e. Whether Defendants failed to implement and maintain reasonable privacy  
22 protections appropriate to the nature and scope of the information collected; and
- 23           f. Whether Class Members are entitled to actual, consequential, and/or nominal  
24 damages and/or injunctive relief as a result of Defendants' wrongful conduct.
- 25  
26  
27

1 106. Finally, all members of the proposed Classes are readily ascertainable. Defendants  
2 have access to Class Members' device identifiers and associated information affected by the  
3 unauthorized data collection that has taken place.

4 107. **Declaratory and Injunctive Relief:** Rules 23(b)(1) and (2) contemplate a class  
5 action for purposes of seeking class-wide injunctive relief. Here Defendants have engaged in  
6 conduct that has uniformly harmed all Fire TV users in the United States. Since Defendants'  
7 conduct has been uniformly directed at all consumers in the United States, and the conduct  
8 continues presently, injunctive relief on a class-wide basis is a viable and suitable solution to  
9 remedy Defendants' continuing misconduct.

10 108. The injunctive Class is properly brought and should be maintained as a class action  
11 under Rule 23(a), satisfying the class action prerequisites of numerosity, commonality, typicality,  
12 and adequacy as above stated.

13 **CAUSES OF ACTION**

14 **COUNT I**

15 **Violation of the Video Privacy Protection Act**

16 **18 U.S.C. § 2710, *et seq.***

17 **(On Behalf of Plaintiffs and the Nationwide Classes)**

18 109. Plaintiffs incorporate by reference and re-allege each and every allegation set forth  
19 above as though fully set forth herein.

20 110. Plaintiffs bring this claim individually and on behalf of the members of the  
21 proposed Nationwide Classes against Defendants.

22 111. The VPPA provides that "a video tape service provider who knowingly discloses,  
23 to any person, personally identifiable information concerning any consumer shall be liable to the  
24 aggrieved person[.]" 18 U.S.C. § 2710(b)(1).

25 112. "Personally-identifiable information" is defined to include "information which  
26 identifies a person as having requested or obtained specific video materials or services from a  
27 video tape service provider." 18 U.S.C. § 2710(a)(3).

1 113. A “video tape service provider” is “any person, engaged in the business, in or  
2 affecting interstate commerce, of rental, sale, or delivery of pre-recorded video cassette tapes or  
3 similar audio visual materials.” 18 U.S.C. § 2710(a)(4).

4 114. Defendants are “video tape service providers” because they provide on-demand  
5 access to prerecorded video content through both third-party apps offered through Fire TVs as  
6 well as their own content provided to Fire TV owners through Amazon Prime Video, Freevee  
7 (formerly IMDb TV), and Fire TV Channels. Defendants are thereby “engag[ing] in the business,  
8 in or affecting interstate or foreign commerce, of rental, sale, or delivery of pre-recorded video  
9 cassette tapes or similar audio visual materials.” 18 U.S.C. § 2710(a)(4).

10 115. Defendants violated the VPPA by knowingly disclosing Plaintiffs’ and Class  
11 Members’ personally identifiable Sensitive Information to advertising partners through the  
12 Amazon advertising platform, without obtaining informed, written consent.

13 116. As a result of Defendants’ violations of the VPPA, Plaintiffs and the Nationwide  
14 Classes are entitled to all damages available under the VPPA including declaratory relief,  
15 injunctive and equitable relief, statutory damages of \$2,500 for each violation of the VPPA, and  
16 attorney’s fees, filing fees, and costs.

17 **COUNT II**

18 **Common Law Invasion of Privacy - Intrusion Upon Seclusion**  
19 **(On Behalf of Plaintiffs and the Nationwide Classes)**

20 117. Plaintiffs incorporate by reference and re-allege each and every allegation set forth  
21 above as though fully set forth herein.

22 118. Plaintiffs bring this claim individually and on behalf of the members of the  
23 proposed Nationwide Classes against Defendants.

24 119. At all relevant times, Plaintiffs and Class Members had a reasonable expectation  
25 that the content they viewed on their Fire TVs in the privacy of their homes would remain private  
26 and would not be surreptitiously monitored, recorded, analyzed, or exploited by Defendants.

1 120. Defendants, without authorization, intentionally intruded upon the seclusion and  
2 private affairs of Plaintiffs and Class Members by secretly installing and operating the ACR Tool  
3 on Fire TVs to continuously monitor and record the content displayed on consumers' screens,  
4 including the specific programs watched, the duration of viewing, and data from externally  
5 connected devices.

6 121. This intrusion was substantial and highly offensive to a reasonable person. The  
7 notion that a television manufacturer and operating system provider would secretly monitor every  
8 image and sound displayed on a consumer's TV screen—and then use that information for  
9 targeted advertising—would be highly offensive and objectionable to any reasonable person.

10 122. The intrusion related to private matters—specifically, Plaintiffs' and Class  
11 Members' media consumption habits, viewing preferences, and other Sensitive Information  
12 displayed on their television screens in the privacy of their homes.

13 123. As a direct and proximate result of Defendants' intrusion upon the seclusion and  
14 private affairs of Plaintiffs and Class Members, Plaintiffs and Class Members have suffered  
15 injuries, including emotional distress, invasion of privacy, and diminution of the value of their  
16 Sensitive Information.

17 **COUNT III**

18 **Violation of the State Consumer Fraud Acts**  
19 **(On Behalf of Plaintiffs and the Multi-State Consumer Fraud Subclass)**

20 124. Plaintiffs incorporate by reference and re-allege each and every allegation set forth  
21 above as though fully set forth herein.

22 125. The Consumer Fraud Acts of the States in the Consumer Fraud Multi-State Class  
23 prohibit the use of unfair or deceptive business practices in the conduct of trade or commerce.

24 126. Plaintiffs have standing to pursue a cause of action for violation of the Consumer  
25 Fraud Acts of the states in the Consumer Fraud Multi-State Class because Plaintiffs and Members  
26 of the Consumer Fraud Multi-State Class have suffered an injury in fact and lost money as a result

1 of Defendants’ actions set forth herein, and because the consumer fraud acts of the states are  
2 substantially similar.

3 127. Defendants engaged in unfair and/or deceptive conduct, including, but not limited  
4 to, monitoring, recording, analyzing, and exploiting the Sensitive Information of Plaintiffs and the  
5 Consumer Fraud Multi-State Class and intentionally concealing the fact of its monitoring,  
6 recording, analyzing, and exploiting of that Sensitive Information.

7 128. Defendants intended that Plaintiffs and each of the other Members of the Consumer  
8 Fraud Multi-State Class would rely upon and be misled their unfair and deceptive conduct and a  
9 reasonable person would in fact be misled by this deceptive conduct described herein.

10 129. As a result of Defendants’ use or employment of unfair or deceptive acts or  
11 business practices, Plaintiffs and each of the other Members of the Consumer Fraud Multi-State  
12 Class have sustained damages in an amount to be proven at trial.

13 130. In addition, Defendants’ conduct showed malice, motive, and the reckless disregard  
14 of the truth such that an award of punitive damages is appropriate.

15 131. Without injunctive relief, Plaintiffs cannot trust that Defendants will truly cease  
16 non-consensual monitoring, recording, analyzing, and exploiting of their Sensitive Information,  
17 and cannot be sure that Defendants will not surreptitiously inject new dark patterns to obscure the  
18 use of their spyware again. Plaintiffs and other members of the Multi-State Class paid good  
19 money for televisions that would not spy on them, and only injunctive relief can give them that  
20 assurance.

21 **COUNT IV**

22 **Violations of the Illinois Consumer Fraud and Deceptive Business Practices Act**  
23 **(On Behalf of Plaintiff Manypenny and the Illinois Subclass)**

24 132. Plaintiff Manypenny incorporates by reference and re-alleges each and every  
25 allegation set forth above as though fully set forth herein.

26 133. Plaintiff and Illinois Subclass members are consumers under the Illinois Consumer  
27 Fraud Act and Defendants are “person[s]” within the meaning of 815 Ill. Comp. Stat. 510/1(5).

1 134. Defendants engaged, and continue to engage, in the wrongful conduct alleged  
2 herein in the course of trade and commerce, as defined in 815 ILCS 505/2 and 815 ILCS 510/2.

3 135. Defendants' representations and omissions concerning the representations were  
4 false and/or misleading as alleged herein.

5 136. Defendants' foregoing deceptive acts and practices, including their omissions, were  
6 likely to deceive, and did deceive, consumers acting reasonably under the circumstances.  
7 Consumers, including Plaintiff and proposed Illinois Subclass Members, would not have  
8 purchased their Product had they known the Products were programmed by design to  
9 surreptitiously spy on them.

10 137. Defendants' false or misleading representations and omissions were such that a  
11 reasonable consumer would attach importance to them in determining his or her purchasing  
12 decision.

13 138. Defendants' false and misleading representations and omissions were made to the  
14 entire Illinois Subclass as they were prominently displayed on the packaging of the Products, the  
15 Defendants' website, and the online pages for the Products.

16 139. Defendants knew or should have known their representations and omissions were  
17 material and were likely to mislead consumers, including Plaintiff and the Illinois Subclass.

18 140. Defendants profited from the sale of the falsely, deceptively, and unlawfully  
19 advertised Products to consumers.

20 141. Defendants' wrongful business practices constituted, and constitute, a continuing  
21 course of conduct in violation of the Illinois Consumer Fraud Act.

22 142. Defendants' wrongful business practices were a direct and proximate cause of  
23 actual harm to Plaintiff and to each Illinois Subclass Member.

24 143. As a direct and proximate result of Defendants' unfair and deceptive trade  
25 practices, Plaintiff and the other Illinois Subclass members have suffered ascertainable loss and  
26 actual damages. Plaintiff and the other Illinois Subclass members who purchased the Products  
27

1 would not have purchased them, or, alternatively, would have paid less for them had the truth  
2 about the Products’ surreptitious spying. Plaintiff and the other Illinois Subclass members did not  
3 receive the benefit of the bargain. Plaintiff and the other Illinois Subclass members are entitled to  
4 recover actual damages, attorneys’ fees and costs, and all other relief allowed under 815 Ill Comp.  
5 Stat. 505/1, *et seq.*

6 144. Without injunctive relief, Plaintiff cannot trust that Defendants will truly cease  
7 non-consensual monitoring, recording, analyzing, and exploiting of their Sensitive Information,  
8 and cannot be sure that Defendants will not surreptitiously inject new dark patterns to obscure the  
9 use of their spyware again. Plaintiffs and other members of the Illinois Subclass paid good money  
10 for televisions that would not spy on them, and only injunctive relief can give them that assurance.

11 **COUNT V**

12 **Violation of New York G.B.L. § 349**  
13 **(On Behalf of Plaintiff Enser and the New York Subclass)**

14 145. Plaintiff Enser incorporates by reference and re-alleges each and every allegation  
15 set forth above as though fully set forth herein.

16 146. Plaintiff and Class members are “persons” within the meaning of the GBL §  
17 349(h).

18 147. Defendants are “person[s], firm[, corporation[s] or association[s] or agent[s] or  
19 employee[s] thereof” within the meaning of GBL § 349(b).

20 148. New York General Business Law Section 349 (“GBL § 349”) declares unlawful  
21 “[d]eceptive acts or practices in the conduct of any business, trade, or commerce or in the  
22 furnishing of any service in this state.”

23 149. Defendants’ deceptive acts and practices include surreptitiously monitoring,  
24 recording, analyzing, and exploiting Plaintiff’s and New York Class Members’ Sensitive  
25 Information without their consent, as well as employing dark patterns to obscure from Plaintiff  
26 and New York Class Members that they were monitoring, recording, analyzing, and exploiting  
27 their Sensitive Information.

1 150. In doing so, Defendants engaged in deceptive acts or practices in violation of GBL  
2 § 349.

3 151. Information as to the ACR spyware functionality of the Products was in  
4 Defendants' exclusive control. Plaintiff and New York Subclass Members did not know that the  
5 Products at issue were sold with Amazon's spyware embedded in them, and Amazon took  
6 affirmative steps to ensure that Plaintiff and New York Subclass Members did not discover this  
7 fact.

8 152. Defendants' deceptive acts and practices are misleading in a material way because  
9 they violate consumers' reasonable expectations. Defendants knew consumers would purchase the  
10 Products and/or pay more for them without knowing that they were spyware devices.

11 153. Defendants' deceptive acts and practices were directed at consumers.

12 154. Defendants' misleading conduct concerns widely purchased consumer products and  
13 affects the public interest. Defendants' conduct includes unfair and misleading acts and practices  
14 that have the capacity to deceive consumers and are harmful to the public at large. Defendants'  
15 conduct is misleading in a material way because consumers do not expect the televisions they buy  
16 will spy on them, and Defendants take advantage of this expectation to surreptitiously monitor,  
17 record, analyze, and exploit consumers' Sensitive Information.

18 155. Plaintiff and New York Subclass members suffered ascertainable loss as a direct  
19 and proximate result of Defendants' GBL violations in that: (i) they would not have purchased the  
20 Products had they known the truth; and (ii) they overpaid for the Products on account of the  
21 misrepresentations and omissions, as described herein. As a result, Plaintiff and New York  
22 Subclass members have been damaged in the difference in value between the Products as  
23 warranted (ordinary televisions) and the Products as actually sold (televisions equipped with  
24 sophisticated surveillance software).

25 156. On behalf of himself and other members of the New York Subclass, Plaintiff seeks  
26 to enjoin Defendants' unlawful acts and practices described herein, to recover actual damages or  
27

1 \$50, whichever is greater, reasonable attorney’s fees and costs, and any other just and proper relief  
2 available under GBL § 349.

3 **COUNT VI**

4 **Violation of New York G.B.L. § 350**  
5 **(On Behalf of Plaintiff Enser and the New York Subclass)**

6 157. Plaintiff Enser incorporates by reference and re-alleges each and every allegation  
7 set forth above as though fully set forth herein.

8 158. GBL § 350 provides that “[f]alse advertising in the conduct of any business, trade  
9 or commerce or in the furnishing of any service in this state is hereby declared unlawful.”

10 159. New York General Business Law Section 350-a(1) defines false advertising as  
11 “advertising, including labeling, of a commodity, or of the kind, character, terms or conditions of  
12 any employment opportunity if such advertising is misleading in a material respect. In  
13 determining whether any advertising is misleading, there shall be taken into account (among other  
14 things) not only representation made by statement, word, design, device, sound or any  
15 combination thereof, but also the extent to which the advertising fails to reveal facts material in  
16 the light of such representations with respect to the commodity or employment to which the  
17 advertising relates under the conditions proscribed in said advertisement, or under such conditions  
18 as are customary or usual.”

19 160. Defendants’ labeling and advertisement of the Products was false and misleading in  
20 a material way. Specifically, Defendants advertised the Products as normal televisions but “fails  
21 to reveal facts material in light of such representations,” namely that the televisions are actually  
22 sophisticated surveillance devices which Defendants employ to monitor, record, analyze, and  
23 exploit Plaintiff’s and New York Subclass Members’ Sensitive Information.

24 161. Plaintiff and New York Subclass Members understood Defendants’  
25 misrepresentations to mean that the Products was an ordinary television, as reasonable consumers  
26 understand the term. Reasonable consumers do not understand a television to be a surveillance  
27 device used to monitor, record, analyze, and exploit their Sensitive Information.

1 162. Defendants' misrepresentations and omissions are consumer-oriented and were and  
2 are likely to mislead reasonable consumers acting reasonably under the circumstances.

3 163. Defendants' misrepresentations and omissions have resulted in consumer injury or  
4 harm to the public interest.

5 164. As a result of the misrepresentations and omissions, Plaintiff and New York  
6 Subclass members have suffered economic injury because: (i) they would not have purchased the  
7 Products had they known the truth; and (ii) they overpaid for the Products on account of the  
8 misrepresentations and omissions, as described herein. As a result, Plaintiff and New York  
9 Subclass members have been damaged in the difference in value between the Products as  
10 warranted (ordinary televisions) and the Products as actually sold (televisions equipped with  
11 sophisticated surveillance software).

12 165. By reason of the foregoing and as a result of Defendants' conduct, Plaintiff and  
13 New York Subclass members seek to enjoin the unlawful acts and practices described herein, to  
14 recover their actual damages or five hundred dollars, whichever is greater, three times actual  
15 damages, reasonable attorneys' fees and costs, and any other just and proper relief available under  
16 GBL § 350.

17 **COUNT VII**

18 **Breach of Implied Contract**  
19 **(On Behalf of Plaintiffs and the National Classes, or in the Alternative,**  
20 **the Nationwide Amazon Fire TV Class)**

21 166. Plaintiffs incorporate by reference and re-allege each and every allegation set forth  
22 above as though fully set forth herein.

23 167. Plaintiffs bring this claim individually and on behalf of the members of the  
24 proposed Nationwide Classes against Defendants.

25 168. When Plaintiffs and Class Members purchased and used Fire TVs, an implied  
26 contract was formed between Plaintiffs and Class Members and Defendants. By purchasing and  
27 using Fire TVs, Plaintiffs and Class Members reasonably expected that the Fire TVs would

1 function as advertised—as entertainment devices for watching television and streaming content—  
2 without surreptitious surveillance and data collection beyond what was clearly disclosed and  
3 consented to.

4 169. In the alternative, when Plaintiff Manypenny and the Nationwide Amazon Fire TV  
5 Class purchased their Amazon-branded Fire TVs directly from Amazon, an implied contract was  
6 formed between Plaintiff and Subclass Members and Defendants. By purchasing and using  
7 Amazon Fire TVs, Plaintiffs and Class Members reasonably expected that the Amazon Fire TVs  
8 would function as advertised—as entertainment devices for watching television and streaming  
9 content—without surreptitious surveillance and data collection beyond what was clearly disclosed  
10 and consented to.

11 170. Defendants had an implied contractual duty to: (a) clearly and conspicuously  
12 disclose the nature and scope of any data collection conducted through the Fire TVs; (b) obtain  
13 informed consent before collecting Sensitive Information through the ACR Tool; and (c) not  
14 collect, use, or monetize Sensitive Information beyond what was necessary to provide the services  
15 for which the Fire TVs were purchased.

16 171. Defendants breached the implied contract by secretly installing and operating the  
17 ACR Tool to collect and monetize Plaintiffs' and Class Members' Sensitive Information without  
18 informed consent, by enabling data collection settings by default, and by designing their user  
19 interface to obscure and minimize the ability of consumers to understand and control the collection  
20 of their data.

21 172. As a direct and proximate result of Defendants' breach, Plaintiffs and Class  
22 Members have suffered damages, including invasion of privacy, loss of the benefit of the bargain,  
23 and diminution of the value of their Sensitive Information.

**COUNT VIII**

**Unjust Enrichment  
(On Behalf of Plaintiffs and the Nationwide Classes)**

1  
2  
3 173. Plaintiffs incorporate by reference and re-allege each and every allegation set forth  
4 above as though fully set forth herein.

5 174. Defendants received a benefit through their surreptitious collection, use, and  
6 monetization of Plaintiffs' and Class Members' Sensitive Information through the ACR Tool.

7 175. This benefit was received at the expense of Plaintiffs and Class Members, who  
8 suffered invasion of privacy, diminution of the value of their Sensitive Information, and loss of the  
9 benefit of the bargain.

10 176. The circumstances make it unjust for Defendants to retain this benefit without  
11 payment to Plaintiffs and Class Members. Defendants collected and monetized Sensitive  
12 Information through deceptive means, without obtaining informed consent, and without providing  
13 any compensation to the consumers whose data they exploited.

14 177. Defendants benefitted financially from the advertising revenues and other  
15 compensation tied to their collection and monetization of Sensitive Information, which enrichment  
16 was unjust in light of Defendants' wrongful conduct.

17 178. Under the circumstances, it would be against equity and good conscience to permit  
18 Defendants to retain the ill-gotten benefits they received from Plaintiffs and the Class as the result  
19 of their surreptitious data collection practices.

20 179. Because Defendants' retention of the non-gratuitous benefit conferred on them by  
21 Plaintiffs and the Class Members is unjust and inequitable, Plaintiffs seek restitution from, and an  
22 order from the Court disgorging all profits, benefits, and other compensation obtained by  
23 Defendants due to their wrongful conduct.

24 **PRAYER FOR RELIEF**

25 WHEREFORE, Plaintiffs respectfully request that the Court grant Plaintiffs and all  
26 members of the proposed Classes the following relief against Defendants:

- 1 (a) For an order certifying the Classes and naming Plaintiffs’ attorneys as Class  
2 Counsel to represent the members of the Classes;
- 3 (b) For an order declaring that Defendants’ conduct violates the statutes referenced  
4 herein;
- 5 (c) For compensatory, statutory, and punitive damages in amounts to be determined by  
6 the Court and/or jury;
- 7 (d) For prejudgment interest on all amounts awarded;
- 8 (e) For an order of restitution and all other forms of equitable monetary relief;
- 9 (f) For injunctive relief requiring Defendants to (i) clearly and conspicuously disclose  
10 the nature and scope of ACR data collection to all Fire TV users; (ii) disable all  
11 ACR data collection settings by default and require affirmative opt-in consent; (iii)  
12 provide a simple, one-step mechanism for consumers to disable all ACR data  
13 collection; and (iv) delete all Sensitive Information collected from Plaintiffs and  
14 Class Members without informed consent;
- 15 (g) For an order awarding Plaintiffs and the Classes their reasonable attorneys’ fees  
16 and expenses and costs of suit; and
- 17 (h) Granting such other and further relief as may be just and proper.

18 **DEMAND FOR TRIAL BY JURY**

19 Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs hereby demand a trial by jury  
20 on all issues so triable.

21 Dated: May 6, 2026

Respectfully submitted,

22 /s/ Roger M. Townsend

23 Roger M. Townsend

**TOWNSEND LEGAL**

380 Winslow Way, Suite 200

Bainbridge Island, WA 98110

Telephone: (206) 761-2649

Email: roger@townsendlegal.com

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  
27

Nick Suciu III (*pro hac vice* forthcoming)  
**BRYSON HARRIS SUCIU & DEMAY PLLC**  
6905 Telegraph Road, Suite 115  
Bloomfield Hills, MI 48301  
Telephone: (616) 678-2180  
Email: nsuciu@brysonpllc.com

Trenton R. Kashima (*pro hac vice* forthcoming)  
**BRYSON HARRIS SUCIU & DEMAY PLLC**  
19800 MacArthur Blvd., Suite 270  
Irvine, CA 92612  
Telephone: (212) 946-9389  
Email: tkashima@brysonpllc.com

*Attorneys for Plaintiffs*