

1 Daniel Srourian, Esq. (SBN 285678)
SROURIAN LAW FIRM, P.C.
2 468 N. Camden Dr. Suite 200
Beverly Hills, CA 90210
3 Telephone: (213) 474-3800
Facsimile: (213) 471-4160
4 Email: daniel@slfla.com

5 *Attorneys for Plaintiffs, Minor*
Plaintiffs, and the Putative Class

7 **UNITED STATES DISTRICT COURT**
CENTRAL DISTRICT OF CALIFORNIA
8 **CIVIL DIVISION**

9 **RAQUEL DIAZ**, on behalf of her minor
child, **B.E.**, and all others similarly
10 situated, **LISA MEDINA**, on behalf of
her minor child, **G.C.**, and all others
11 similarly situated, **OSCAR**
RODRIGUEZ, on behalf of his minor
12 child, **F.R.**, and all others similarly
situated, **STACY RADER**, on behalf of
13 her minor child, **S.C.**, and **KATRINA**
MONTGOMERY, on behalf of her
14 minor children, **J.M.**, **J.A.**, and **J.M.**,
and all others similarly situated,

15 Plaintiffs,

16 v.

17 **PARAMOUNT SKYDANCE**
18 **CORPORATION and PLUTO INC.**,

19 Defendants.

Case No.

JURY TRIAL DEMANDED

1 **CLASS ACTION COMPLAINT**

2 Plaintiffs Raquel Diaz, Lisa Medina, Oscar Rodriguez, Stacy Rader, and Katrina
3 Montgomery on behalf of their minor children, B.E., G.C., F.R., S.C., J.M., J.A., and
4 J.M. (the “**Plaintiffs’ Children**”), and all similarly situated persons, allege the following
5 against Defendants Paramount Skydance Corporation (“**Paramount**”) and Pluto Inc.
6 (“**Pluto**” and together with Paramount, “**Defendants**”), based upon personal knowledge
7 with respect to themselves and their children, and on information and belief derived
8 from, among other things, investigation by Plaintiffs’ counsel and review of public
9 documents as to all other matters:

8 **I. INTRODUCTION**

9 1. Protecting children’s privacy is a major concern for parents in this
10 interconnected age. In a recent survey, more than 85% of parents believe that access to
11 technology is important for their children’s future, but more than three quarters of
12 parents are concerned about protecting their family’s security, and 73% were concerned
13 about their children’s personal data being collected by third parties, without their
14 consent.¹

15 2. These concerns are well founded. “[U]p until age 18, young people are
16 highly vulnerable to advertising.”² In the words of one researcher:

17
18 There’s a lot of neuroscience that explains why adolescents and children
19 are so vulnerable [to advertising]...they’re much more attuned to rewards,
20 much less attentive to consequences and risks, much more tolerant of
21 ambiguity, much more sensitive to social cues and much more impulsive,

18 ¹ *POLLING MEMO: PARENTS’ VIEWS ON CHILDREN’S DIGITAL PRIVACY AND SAFETY, TRUSTED*
19 *FUTURE*, <https://trustedfuture.org/childrens-digital-privacy-and-safety/#:~:text=87%25%20of%20parents%20believe%20technology,the%20lives%20of%20their%20parents>
(last visited Feb. 25, 2025).

20 ² *Exposing the Dangers of Targeting Children as Consumers*, UC IRVINE PAUL MERAGE SCHOOL OF BUSINESS
21 (July 3, 2024), <https://merage.uci.edu/news/2024/07/Exposing-the-Dangers-of-Targeting-Children-as-Consumers.html> (last visited Aug. 1, 2025).

1 so they don't have a lot of cognitive control...*This is an advertiser's*
2 *dream.*³

3 3. Given these concerns, one would hope that websites catering to children
4 would be especially careful to avoid sharing information about those children with
5 advertisers, or at the very least, to be upfront with parents about the information they
6 give away, so parents can decide whether the website is appropriate. Unfortunately, that
7 is sometimes not the case.

8 4. Unbeknownst to those viewers and their parents, including Plaintiffs and
9 their children, Defendants have chosen to harvest personally identifiable information on
10 its child-directed video platform, including the specific videos watched by minors (the
11 "**Private Children's Data**"), and contemporaneously shares that information with
12 internet advertising giants, including Alphabet, Inc. ("**Google**") and Microsoft Corp.
13 ("**Microsoft**").

14 5. Defendant Paramount is a multinational mass media company that provides
15 network, studio, and streaming content to over 1-billion subscribers worldwide through
16 its many well-known brands, including CBS, MTV, Comedy Central, Nickelodeon,
17 Showtime, and Paramount Pictures.⁴ Pluto is a Paramount subsidiary operating the Pluto
18 TV video streaming service, which provides its users with access to over 700,000 hours
19 of pre-recorded video content, including a wide-variety of child-friendly programming

20 ³ *Id.*

21 ⁴ *About*, PARAMOUNT, <https://www.paramount.com/about> (last visited Aug. 1, 2025); *Brands*, PARAMOUNT, <https://www.paramount.com/brands> (last visited Aug. 1, 2025).

1 hosted in Pluto TV’s specific “Kids” section.⁵ This content is accessed by viewers
2 through Defendants’ online video streaming platform, available by either visiting
3 www.pluto.tv, or downloading one of Defendants’ many mobile phone, tablet, and
4 desktop applications (the “**Platform**”).⁶ To use the Platform through an application,
5 users must first sign-up for a Pluto TV account.

6 6. Giants like Google and Microsoft compile Defendants’ information as fuel
7 for their targeted advertising enterprise. That data is then used to stream ads to
8 Defendants’ customers. When Google and Microsoft receive information about an
9 individual’s media preferences and educational attainment, they compile it into an ever-
10 growing advertising profile specific to the individual which they use to stream tailored
11 ads to that person’s computers and smartphones based on the individual’s demography,
12 interests, goals, and anxieties.

13 7. One of the ways that Google and Microsoft gather this information is
14 through offering web service operators a *quid pro quo*. Google and Microsoft offer web
15 operators access to their proprietary suites of marketing, advertising, and customer
16 analytics software, including Google Analytics, Google AdSense, Google Tag Manager,
17 Microsoft Advertising, Big Ads, and Xandr (collectively, the “**Business Tools**”). Armed
18 with these Business Tools, web service operators can leverage Google and Microsoft’s

19
20 _____
⁵ Pluto TV, PARAMOUNT, <https://www.paramount.com/brands/pluto-tv> (last visited Aug. 1, 2025).

⁶ See *Where to Watch*, PLUTO TV, <https://pluto.tv/where-to-watch> (last visited Aug. 1, 2025).

1 enormous database of consumer information for the purposes of deploying targeted
2 advertisements, performing minute analyses of their customer bases, and identifying
3 new market segments that may be exploited.

4 8. But, in exchange for access to these Business Tools, web service operators
5 install Google and Microsoft’s surveillance software on their website (the “Tracking
6 Tools”), including ‘tracking pixels’ (“**Pixels**”) and third-party ‘cookies’ that capture
7 sensitive, personally identifiable information provided to the website operator by its
8 website users. This sensitive information can include a unique identifier that Google and
9 Microsoft use to identify that user, regardless of what computer or phone is used to
10 access the website. The Tracking Tools can also capture and share other information like
11 the specific webpages visited by a website user, items added to an online shopping cart
12 by a website user, information entered into an online form by a website user, and the
13 device characteristics of a website user’s phone or computer.

14 9. In essence, when website operators use Google and Microsoft’s Business
15 Tools, they choose to participate in Google and Microsoft’s mass surveillance network
16 and, in turn, benefit from Google and Microsoft’s collection of user data at the expense
17 of their customers’ privacy.

18 10. Defendants have chosen to prioritize their marketing efforts over consumer
19 privacy by installing Google and Microsoft’s Tracking Tools on its website, including in
20 the “Kids” section.

21

1 11. Each of the Plaintiffs’ Children and Class Members visited the Platform and
2 had their Private Children’s Data tracked by Defendants using the Tracking Tools.
3 However, Defendants *never* obtained authorization from Plaintiffs or Class Members to
4 share the Private Children’s Data they collect with third parties. At all times relevant to
5 this action, Plaintiffs and Class Members gave no informed consent for the Private
6 Children’s Data to be transmitted to third parties, including two of the largest advertisers
7 and compilers of user information in the world

8 12. Moreover, Defendants’ tracking of users violated numerous state and
9 federal laws, including the Video Privacy Protection Act (“**VPPA**”), passed specifically
10 to prevent the disclosure and aggregation of data relating to an individual’s video
11 consumption, and the Children’s Online Privacy Protection Act of 1998 (“**COPPA**”),
12 enacted to protect children, like Plaintiffs’ Children, from being surveilled while using
13 the Internet.

14 13. As a result of Defendants’ conduct, Plaintiffs, Plaintiffs’ Children and Class
15 Members have suffered numerous injuries, including: (i) invasion of privacy; (ii) lack of
16 trust in communicating with online service providers; (iii) emotional distress and
17 heightened concerns related to the release of the Private Children’s Data to third parties,
18 (iv) loss of benefit of the bargain; (v) diminution of value of the Private Children’s Data;
19 and (vi) statutory damages.

1 14. Therefore, Plaintiffs seek, on behalf of Plaintiffs’ Children and a class of
2 similarly situated persons, to remedy these harms and assert the following statutory and
3 common law claims against Paramount: violations of the Video Privacy Protection Act,
4 18 U.S.C. § 2710, *et seq.*; Invasion of Privacy; violations of the Electronic
5 Communications Privacy Act, 18 U.S.C. § 2511(1), *et seq.*; violations of the California
6 Invasion of Privacy Act, Cal. Pen. Code § 360, *et seq.*; Invasion of Privacy Under
7 California’s Constitution, Cal. Const. Art. 1, § 1; Negligence; Breach of Implied
8 Contract; and Unjust Enrichment.

9 **II. PARTIES**

10 ***Plaintiff Raquel Diaz and Minor Plaintiff B.E.***

11 15. Plaintiff Diaz and Minor Plaintiff B.E. are citizens of the State of
12 California, residing in San Bernardino County. Plaintiff Diaz brings this action on behalf
13 of Minor Plaintiff B.E., and all others similarly situated.

14 16. In 2025, Minor Plaintiff B.E. utilized Defendants’ Platform on the family’s
15 personal electronic devices to watch pre-recorded video content hosted in the “Kids”
16 section of Defendants’ Platform.

17 17. Plaintiff Diaz never authorized Defendants to disclose any aspect of Minor
18 Plaintiff B.E.’s use of their platform to third parties, including the Private Children’s
19 Data that Minor Plaintiff B.E. provided to Defendants by using the Platform.

1 18. On every occasion that she viewed child-directed video content on the
2 Platform, Minor Plaintiff B.E. was under the age of thirteen, possessed accounts with
3 Google and Microsoft, and accessed Defendants' Platform while logged into those
4 Google and Microsoft accounts on the same device.

5 ***Plaintiff Lisa Medina and Minor Plaintiff G.C.***

6 19. Plaintiff Medina and Minor Plaintiff G.C. are citizens of the State of
7 Illinois, residing in Cook County. Plaintiff Medina brings this action on behalf of Minor
8 Plaintiff G.C., and all others similarly situated.

9 20. In 2025, Minor Plaintiff G.C. utilized Defendants' Platform on the family's
10 personal electronic devices to watch pre-recorded video content hosted in the "Kids"
11 section of Defendants' Platform.

12 21. Plaintiff Medina never authorized Defendants to disclose any aspect of
13 Minor Plaintiff G.C.'s use of their platform to third parties, including the Private
14 Children's Data that Minor Plaintiff G.C. provided to Defendants by using the Platform.

15 22. On every occasion that Minor Plaintiff G.C. viewed child-directed video
16 content on the Platform, Minor Plaintiff G.C. was under the age of thirteen, possessed
17 accounts with Google and Microsoft, and accessed Defendants' Platform while logged
18 into those Google and Microsoft accounts on the same device.

19
20
21

1 ***Plaintiff Oscar Rodriguez and Minor Plaintiff F.R.***

2 23. Plaintiff Rodriguez and Minor Plaintiff F.R. are citizens of the State of
3 Illinois, residing in LaSalle County. Plaintiff Rodriguez brings this action on behalf of
4 Minor Plaintiff F.R., and all others similarly situated.

5 24. In or around 2024, Minor Plaintiff F.R. utilized Defendants' Platform on
6 the family's personal electronic devices to watch pre-recorded video content hosted in
7 the "Kids" section of Defendants' Platform.

8 25. Plaintiff Rodriguez never authorized Defendants to disclose any aspect of
9 Minor Plaintiff F.R.'s use of their platform to third parties, including the Private
10 Children's Data that Minor Plaintiff F.R. provided to Defendants by using the Platform.

11 26. On every occasion that he viewed child-directed video content on the
12 Platform, Minor Plaintiff F.R. was under the age of thirteen, possessed accounts with
13 Google and Microsoft, and accessed Defendants' Platform while logged into those
14 Google and Microsoft accounts on the same device.

15 ***Plaintiff Stacy Rader and Minor Plaintiff S.C.***

16 27. Plaintiff Rader and Minor Plaintiff S.C. are citizens of the State of New
17 Jersey, residing in Middlesex County. Plaintiff Rader brings this action on behalf of
18 Minor Plaintiff S.C., and all others similarly situated.

19
20
21

1 28. In or around September of 2024, Minor Plaintiff S.C. utilized Defendants'
2 Platform on the family's personal electronic devices to watch pre-recorded video content
3 hosted in the "Kids" section of Defendants' Platform.

4 29. Plaintiff Rader never authorized Defendants to disclose any aspect of Minor
5 Plaintiff S.C.'s use of their platform to third parties, including the Private Children's
6 Data that Minor Plaintiff S.C. provided to Defendants by using the Platform.

7 30. On every occasion that he viewed child-directed video content on the
8 Platform, Minor Plaintiff S.C. was under the age of thirteen, possessed accounts with
9 Google and Microsoft, and accessed Defendants' Platform while logged into those
10 Google and Microsoft accounts on the same device.

11 ***Plaintiff Katrina Montgomery and Minor Plaintiffs J.M., J.A., and J.M.***

12 31. Plaintiff Montgomery and Minor Plaintiffs J.M., J.A., and J.M. are citizens
13 of the State of Indiana, residing in Marion County. Plaintiff Montgomery brings this
14 action on behalf of Minor Plaintiffs J.M., J.A., and J.M., and all others similarly situated.

15 32. In or around 2024, Minor Plaintiffs J.M., J.A., and J.M. utilized Defendants'
16 Platform on the family's personal electronic devices to watch pre-recorded video content
17 hosted in the "Kids" section of Defendants' Platform.

18 33. Plaintiff Montgomery never authorized Defendants to disclose any aspect
19 of Minor Plaintiffs J.M., J.A., and J.M.'s use of their platform to third parties, including
20
21

1 the Private Children’s Data that Minor Plaintiffs J.M., J.A., and J.M. provided to
2 Defendants by using the Platform.

3 34. On every occasion that he viewed child-directed video content on the
4 Platform, Minor Plaintiffs J.M., J.A., and J.M. were under the age of thirteen, possessed
5 accounts with Google and Microsoft, and accessed Defendants’ Platform while logged
6 into those Google and Microsoft accounts on the same device.

7 ***Defendant Paramount Skydance Corporation***

8 35. Defendant Paramount is a for-profit corporation incorporated in the State
9 of Delaware, with its principal place of business at 5555 Melrose Avenue, Los
10 Angeles, California, in Los Angeles County.

11 ***Defendant Pluto Inc.***

12 36. Defendant Pluto is a for-profit corporation incorporated in the State of
13 Delaware, with its principal place of business at 700 N. San Vicente Boulevard, 9th
14 Floor, West Hollywood, CA, in Los Angeles County.

15 **III. JURISDICTION AND VENUE**

16 37. This Court has subject matter jurisdiction pursuant to the Class Action
17 Fairness Act of 2005 (“CAFA”), 28 U.S.C. § 1332(d). The amount in controversy
18 exceeds the sum of \$5,000,000 exclusive of interest and costs, there are more than 100
19 putative class members and minimal diversity exists because Plaintiffs and many
20 putative class members are citizens of a different state than Defendants. This Court also
21

1 has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged
2 herein form part of the same case or controversy.

3 38. This Court has federal question jurisdiction under 28 U.S.C. § 1331 because
4 this Complaint alleges question of federal laws under the VPPA (18 U.S.C. § 2710, *et*
5 *seq.*) and ECPA (18 U.S.C. § 2511, *et seq.*).

6 39. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. §
7 1367(a) because all claims alleged herein from part of the same case or controversy.

8 40. This Court has personal jurisdiction over Defendants because Defendants
9 operate and maintain their principal places of business in this District. Further,
10 Defendants are authorized to, and regularly conduct business in, this District and make
11 decisions regarding corporate governance and management of the Platform in this
12 District, including decisions regarding the privacy of user's Private Children's Data and
13 the incorporation of the Tracking Tools.

14 41. Venue is proper in this District under 28 U.S.C. § 1391(a)-(d) because: a
15 substantial part of the events giving rise to this action occurred in this District, including
16 decisions made by Defendants' governance and management personnel or inaction by
17 those individuals that led to the unauthorized sharing of Plaintiffs' Children' Private
18 Children's Data; Defendants' principal places of business are located in this District;
19 Defendants collect and redistribute Class Members' Private Children's Data in this

1 District; and Defendants caused harm to Class Members residing in this District,
2 including Minor Plaintiff B.E.

3 **IV. FACTUAL ALLEGATIONS**

4 **A. THE CHILDREN’S ONLINE PRIVACY PROTECTION ACT OF 1998**

5 42. Congress passed COPPA in 1998 to codify the societal expectations of
6 privacy with regards to minor children’s usage of the Internet. COPPA is intended to
7 “maintain the security of personally identifiable information of children collected
8 online” and to “protect children’s privacy by limiting the collection of personal
9 information from children without parental consent.”⁷

10 43. COPPA “prohibits unfair ... acts or practices in connection with the
11 collection, use, and/or disclosure of personal information from and about children on the
12 Internet.” 16 C.F.R. § 312.1. Moreover, COPPA specifically prohibits “an operator of a
13 website or online service...[from] collect[ing] personal information from a child in a
14 manner that violates the regulations prescribed [by the Federal Trade Commission
15 (“FTC”)]” where the website or online service is “directed to children” or the website
16 operator “has actual knowledge that it is collecting personal information from a child[.]”
17 15 U.S.C. § 6502.

18 44. When passed in 1998, COPPA defined “personal information” as meaning:

19 _____
20 ⁷ *Dissenting Statement of FTC Commissioner Rebecca Kelly Slaughter In the Matter of Google LLC and*
YouTube, LLC, FEDERAL TRADE COMMISSION (Sep. 9, 2019), available online at:
21 https://www.ftc.gov/system/files/documents/public_statements/1542971/slaughter_google_youtube_statement.pdf.

1 individually identifiable information about an individual collected online,
2 including--(A) a first and last name; (B) a home or other physical address
3 including street name and name of a city or town; (C) an e-mail address;
4 (D) a telephone number; (E) a Social Security number; (F) any other
5 identifier that the Commission determines permits the physical or online
6 contacting of a specific individual; or (G) information concerning the child
7 or the parents of that child that the website collects online from the child
8 and combines with an identifier described in this paragraph.

9 15 USCS § 6501 (1998).

10 45. Then, in 2013, COPPA was enhanced, and its definition of “personal
11 information” was widened to explicitly include “persistent identifier[s] that can be used
12 to recognize a user over time and across different Web sites or online services” including
13 “customer number[s] held in a cookie,” “Internet Protocol (IP) address[es],” “processor
14 or device serial number[s],” and “unique device identifier[s].” 16 C.F.R. § 312.2.

15 46. To comply with COPPA, website operators collecting information from
16 children must:

17 provide notice on the website of what information is collected from
18 children by the operator, how the operator uses such information, and the
19 operator’s disclosure practices for such information; and ... obtain
20 verifiable parental consent for the collection, use, or disclosure of personal
21 information from children[.]

15 U.S.C. § 6502(b)(1)(A).

47. In order to determine whether a website or online service is “directed to
children” the FTC considers the website’s:

subject matter, visual content, use of animated characters or child-oriented
activities and incentives, music or other audio content, age of models,
presence of child celebrities or celebrities who appeal to children, language

1 or other characteristics of the Web site or online service, as well as whether
2 advertising promoting or appearing on the Web site or online service is
directed to children.

3 16 CFR § 312.2.

4 48. The video content watched by Plaintiffs' Children on the Platform is
5 obviously "directed to children" under the meaning of COPPA, as it consists of
6 television shows and movies explicitly produced for a child audience, and hosted by
7 Defendants on the "Kids" section of the Platform.

8 49. Accordingly, Defendants' collection and disclosure of personally
9 identifiable information without obtaining parental permission from minor users of the
10 Platform, like Plaintiffs' Children, constitutes a violation of COPPA.

11 **B. THE VIDEO PRIVACY PROTECTION ACT**

12 50. The VPPA was passed in 1988 in response to Congress's concern that "the
13 trail of information generated by every transaction that is now recorded and stored in
14 sophisticated record-keeping systems is a new, more subtle and pervasive form of
15 surveillance." S. Rep. No. 100-599, at p. 7 (1988) (statement of Sen. Patrick Leahy).

16 51. In passing the VPPA, Congress was particularly alarmed about surveillance
17 of Americans' media consumption, recognizing that:

18 Books and films are the intellectual vitamins that fuel the growth of
19 individual thought. The whole process of intellectual growth is one of
20 privacy-of quiet, and 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.

21

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

2 52. Although the VPPA was originally intended to protect the privacy of an
3 individual’s rental videotape selections, Congress has repeatedly reiterated that the
4 VPPA is applicable to “‘on-demand’ cable services and Internet streaming services
5 [that] allow consumers to watch movies or TV shows on televisions, laptop computers,
6 and cell phones.” S. Rep. 112-258, at p. 2.⁸

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

12 54. The VPPA defines a “video tape service provider” as “any person, engaged
13 in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery
14 of pre-recorded video cassette tapes or similar audio-visual materials.” 18 U.S.C. §
15 2710(a)(4).

16
17
18 _____
19 ⁸ See also *The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century*, SENATE JUDICIARY,
20 SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW (Jan. 31, 2012), available online at
21 <https://www.judiciary.senate.gov/download/hearing-transcript-the-videoprivacy-protection-act-protecting-viewer-privacy-in-the-21st-century> (statement by Senator Leahy, who originally introduced the VPPA in the Senate: “Now, it is true that technology has changed...but I think we should all agree that we have to be faithful to our fundamental right to privacy and freedom. Today the social networking, video streaming, the cloud, mobile apps, and other new technologies have revolutionized the availability of Americans’ information.”).

1 55. The VPPA additionally defines “personally identifiable information” as
2 “information which identifies a person as having requested or obtained specific video
3 materials or services from a video service provider.” 18 U.S.C. § 2710(a)(3).

4 56. Defendants are inarguably video tape service providers under the meaning
5 of the VPPA. Paramount’s primary business is delivering video content to “audiences
6 across platforms worldwide...through [its] studios, networks, [and] streaming
7 services[.]”⁹ And Pluto TV, Pluto’s sole product, is a video streaming service hosting
8 700,000 hours of pre-recorded content.¹⁰ Accordingly, Defendants’ disclosure of the
9 specific videos viewed by users of the Platform, like Plaintiffs’ Children, constitutes a
10 violation of VPPA. *See, e.g., Fan v. NBA Props. Inc.*, No. 23-cv-05069-SI, 2024 U.S.
11 Dist. LEXIS 57205, at *9 (N.D. Cal. Mar. 26, 2024) (“in enacting the VPPA,
12 ‘Congress[] inten[ded] to cover new technologies for pre-recorded video content’” and
13 “used ‘similar audio visual materials’ to ensure that VPPA’s protections would retain
14 their force even as technologies evolve”).

15
16
17
18
19
20 _____
⁹ *About*, PARAMOUNT, <https://www.paramount.com/about> (last visited Aug. 1, 2025).

21 ¹⁰ *Pluto TV*, PARAMOUNT, <https://www.paramount.com/brands/pluto-tv> (last visited Aug. 1, 2025).

1 **C. DEFENDANTS’ USE OF THIRD-PARTY TRACKING**
2 **TECHNOLOGIES**

3 **i. Google and Microsoft’s Mass Advertising Surveillance Operation**

4 57. Google is the largest digital advertiser in the country, accounting for 26.8-
5 percent of the total digital advertising revenue generated in the United States.¹¹ In 2023,
6 Google’s advertising revenue of \$238 billion accounted for 77-percent of its total
7 revenue for the year.¹²

8 58. Google advertises Google Analytics and other Business Tools to web
9 service operators, like Defendants, claiming they will allow the operator to
10 “[u]nderstand [their] site and app users,” “check the performance of [their] marketing,”
11 and “[g]et insights only Google can give.”¹³ But, in order for operators to get information
12 from Google Analytics about their website’s visitors, they must allow data collection
13 through installation of Google’s Tracking Tools on their website.¹⁴

14
15 ¹¹ *Share of major ad-selling companies in digital advertising revenue in the United States*, STATISTA (May 2024),
16 <https://www.statista.com/statistics/242549/digital-ad-market-share-of-major-ad-selling-companies-in-the-us-by-revenue/#:~:text=In%202023%2C%20Google%20accounted%20for,21.1%20and%2012.5%20percent%2C%20respectively> <https://www.scientificamerican.com/article/7-in-10-smartphone-apps-share-your-data-with-third-party-services/> (last visited Aug. 1, 2025).

17
18 ¹² Florian Zandt, *Google’s Ad Revenue Dwarfs Competitors*, STATISTA (Sep. 10, 2024),
19 <https://www.statista.com/chart/33017/annual-advertising-revenue-of-selected-tech-companies-offering-search-solutions/#:~:text=Online%20advertising&text=Alphabet%2C%20the%20company%20behind%20the,overall%20revenue%20this%20past%20year> (last visited Aug. 1, 2025).

20 ¹³ *Welcome to Google Analytics*, GOOGLE, <https://analytics.google.com/analytics/web/provision/?authuser=0#/provision> (last visited Aug. 1, 2025).

21 ¹⁴ See Aaron Ankin & Surya Matta, *The High Privacy Cost of a “Free” Website*, THE MARKUP, <https://themarkup.org/blacklight/2020/09/22/blacklight-tracking-advertisers-digital-privacy-sensitive-websites> (last visited Aug. 1, 2025).

1 59. Indeed, on its *Privacy & Terms* page, Google admits that it collects
2 information from third party websites, stating that “[m]any websites and apps use
3 Google services to improve their content and keep it free. When they integrate our
4 services, these sites and apps share information with Google.”¹⁵

5 60. Google also admits that it uses the information collected from third party
6 websites, such as Defendants’, to sell targeted advertising, explaining to users that, “[f]or
7 example, a website that sells mountain bikes might use Google's ad services. After you
8 visit that site, you could see an ad for mountain bikes on a different site that shows ads
9 served by Google.”¹⁶

10 61. Microsoft is the largest software company in the world, offering a diverse
11 portfolio of product offerings including the Windows operating system, Office 365
12 software suite, LinkedIn professional social networking site, Xbox video gaming
13 platform, as well as numerous targeted advertising products.¹⁷ In 2024, Microsoft
14 generated over \$77-billion in revenue, including \$12-billion derived from its advertising
15 products.¹⁸

16 62. Microsoft markets its Business Tools to website operators, claiming that
17 that its Business Tools can “consolidate user behavior and uncover[] trends, so we can
18

19 ¹⁵ *Privacy & Terms – How Google uses information from sites or apps that use our services*, GOOGLE,
<https://policies.google.com/technologies/partner-sites> (last visited Aug. 1, 2025).

20 ¹⁶ *Id.*

21 ¹⁷ *Annual Report 2024*, MICROSOFT (Oct. 18, 2024), available online at:
www.microsoft.com/investor/reports/ar24/.

¹⁸ *Id.*

1 make your website better together for retail, content publishers, small business owners,
2 and everywhere in between.”¹⁹

3 63. But, like with Google, website operators using Microsoft’s Business Tools
4 must install Microsoft’s Tracking Tools on their website. Microsoft readily admits that
5 it:

6 generates a unique advertising ID for each person using a device, which
7 app developers and advertising networks can then use for their own
8 purposes, including providing relevant advertising in apps...Microsoft
9 apps and third-party apps can access and use the advertising ID in much the
10 same way that websites can access and use a unique identifier stored in a
11 cookie. Thus, your advertising ID can be used by app developers and
12 advertising networks to provide more relevant advertising and other
13 personalized experiences across their apps and on the web.²⁰

14 64. While Google and Microsoft admit that they collect information from third-
15 party websites through the Tracking Tools, neither provides, nor could provide, a
16 publicly available list of every webpage on which their Tracking Tools are installed. As
17 such, the vague descriptions of Google and Microsoft’s data collection practices
18 referenced above could not give Plaintiffs and Class Members any reason to think that
19 Defendants were part of Google and Microsoft’s surveillance network. Moreover, as
20 Defendants do not disclose their use of Google and Microsoft’s Tracking Tools, Plaintiffs
21 and Class Members could not have been reasonably expected to review any of Google
and Microsoft’s privacy statements in connection with their use of the Platform.

¹⁹ Clarity, MICROSOFT, <https://clarity.microsoft.com/> (last visited Aug. 1, 2025)

²⁰ *Microsoft Privacy Statement*, MICROSOFT, <https://www.microsoft.com/en-us/privacy/privacystatement#mainadvertisingidmodule> (last visited Aug. 1, 2025).

1 65. Google and Microsoft aggregate the user information that they collect from
2 third-party websites into ‘advertising profiles’ consisting of all of the data that they have
3 collected about a given user.²¹ With these advertising profiles, Google and Microsoft can
4 sell hyper-precise advertising services, allowing their clients to target internet users
5 based on combinations of their location, age, race, interests, hobbies, life events (e.g.,
6 recent marriages, graduation, or relocation), political affiliation, education level, home
7 ownership status, marital status, household income, type of employment, use of specific
8 apps or websites, and more.²²

9 66. In fact, Google and Microsoft value user information so highly that they
10 provide their Business Tools to many website operators for free, all to expand their
11 surveillance apparatus.²³

12 67. When website operators, like Defendants, make use of Google and
13 Microsoft’s Business Tools, they are essentially choosing to participate in Google and
14 Microsoft’s mass surveillance network, and in return they benefit from Google and
15 Microsoft’s collection of user data, at the expense of their website users’ privacy. For
16

17 ²¹ Bennett Cyphers & Gennie Gebhart, *Behind the One-Way Mirror: A Deep Dive Into the Technology of*
Corporate Surveillance, ELECTRONIC FRONTIER FOUNDATION (2019), available online at:
18 [https://www.eff.org/files/2019/12/11/behind_the_one-way_mirror-](https://www.eff.org/files/2019/12/11/behind_the_one-way_mirror-a_deep_dive_into_the_technology_of_corporate_surveillance_0.pdf)
[a_deep_dive_into_the_technology_of_corporate_surveillance_0.pdf](https://www.eff.org/files/2019/12/11/behind_the_one-way_mirror-a_deep_dive_into_the_technology_of_corporate_surveillance_0.pdf).

19 ²² *About audience segments*, GOOGLE ADS, [https://support.google.com/google-](https://support.google.com/google-ads/answer/2497941?hl=en#zippy=%2Cin-market-segments%2Caffinity-segments%2Clife-events%2Cdetailed-demographics)
[ads/answer/2497941?hl=en#zippy=%2Cin-market-segments%2Caffinity-segments%2Clife-](https://support.google.com/google-ads/answer/2497941?hl=en#zippy=%2Cin-market-segments%2Caffinity-segments%2Clife-events%2Cdetailed-demographics)
[events%2Cdetailed-demographics](https://support.google.com/google-ads/answer/2497941?hl=en#zippy=%2Cin-market-segments%2Caffinity-segments%2Clife-events%2Cdetailed-demographics) (last visited Aug. 1, 2025).

20 ²³ *Analytics Overview*, GOOGLE, <https://marketingplatform.google.com/about/analytics/> (last visited Aug. 1,
21 2025) (“Google Analytics gives you the tools, free of charge”); *Clarity*, MICROSOFT,
<https://clarity.microsoft.com/> (last visited Aug. 1, 2025) (“Enjoy all the features of Clarity at absolutely zero
cost. You’ll never run into traffic limits or be forced to upgrade to a paid version”).

1 example, in exchange for allowing it to collect user information, Microsoft allows
2 website operators to target customers using “custom data about users” that Microsoft
3 collects from its other clients.²⁴ Likewise, Google rewards website operators for
4 providing it with their user’s information by granting access to its Analytics platform,
5 which leverages demographic data collected by Google to provide detailed analyses of
6 the website’s user base.²⁵

7 **ii. Children Are Specifically Targeted by Online Advertisers**

8 68. Children are not exempted from this mass surveillance machine. As
9 reported by Vox:

10 [T]oday’s kids are the most at risk because they have the largest digital
11 footprint in history. Between the Nest cameras watching kids at home, kids’
12 games that target them with ads, and purchase preferences on Amazon and
13 Google, their data is being harvested at an unprecedented rate.²⁶

14 69. Why are advertisers willing to potentially violate COPA to collect data from
15 minors? The answer is simple: children are particularly susceptible to advertising.

16 70. Indeed, research conducted by the American Academy of Pediatrics has
17 found that “[c]hildren are uniquely vulnerable to the persuasive effects of advertising

18 ²⁴ *Key-Value Targeting*, MICROSOFT, <https://learn.microsoft.com/en-us/xandr/invest/key-value-targeting> (last
19 visited Aug. 1, 2025).

20 ²⁵ *Google Marketing Platform – Features*, GOOGLE, <https://marketingplatform.google.com/about/analytics/features/> (last visited Aug. 1, 2025).

21 ²⁶ Chavie Lieber, *Big tech has your kid’s data — and you probably gave it to them* VOX (Dec. 5, 2018),
<https://www.vox.com/the-goods/2018/12/5/18128066/children-data-surveillance-amazon-facebook-google-apple> (last visited Aug. 1, 2025).

1 because of immature critical thinking skills and impulse inhibition.”²⁷ As one expert
2 explains:

3 There’s a lot of neuroscience that explains why adolescents and children
4 are so vulnerable [to advertising]...they’re much more attuned to rewards,
5 much less attentive to consequences and risks, much more tolerant of
6 ambiguity, much more sensitive to social cues and much more impulsive,
7 so they don’t have a lot of cognitive control...*This is an advertiser’s*
8 *dream.*²⁸

9 71. In pursuit of this dream, advertisers spend more and more on advertising to
10 children every year. In 2023, United States kids’ advertising expenditures totaled nearly
11 **\$3-billion** – by 2031, that number is projected to reach **\$21-billion.**²⁹

12 72. As a result, the National Financial Educators Council notes that:

13 By the time they turn 21, young people will have been exposed to over one
14 million advertisements – many of which are highly-sophisticated ads that
15 encourage them to make purchases based on wants rather than needs.³⁰

16 73. But, if the tactics used by online advertisers are cause for alarm, the
17 products pushed onto children through those tactics are worthy of outright panic.

18 74. Researchers have found that exposure to “newer forms of digital
19 marketing” driven by “data collection” and “personalized behavioral marketing driven
20

21 ²⁷ Jenny Radesky, Yolanda Linda Reid Chassiakos, Nusheen Ameenuddin & Dipesh Navsaria, *Digital Advertising to Children*, 146 PEDIATRICS 1681 (Jul. 2020), available online at: <https://pubmed.ncbi.nlm.nih.gov/32571990/>.

²⁸ *Exposing the Dangers of Targeting Children as Consumers*, UC IRVINE PAUL MERAGE SCHOOL OF BUSINESS (July 3, 2024), <https://merage.uci.edu/news/2024/07/Exposing-the-Dangers-of-Targeting-Children-as-Consumers.html> (last visited Aug. 1, 2025).

²⁹ *Stop Advertising to Kids – Stop Predatory Advertising*, NATIONAL FINANCIAL EDUCATORS COUNCIL, <https://www.financialeducatorsCouncil.org/stop-advertising-to-kids/> (last visited Feb. 25, 2025).

³⁰ *Id.*

1 by machine learning,” is “associated with unhealthy behaviors, such as intake of high-
2 calorie, low-nutrient food and beverages; use of tobacco products and electronic
3 cigarettes; use of alcohol and marijuana; and indoor tanning.”³¹

4 75. The resulting harm to our children is staggering. To take one of many
5 examples, in 1971, cigarettes were banned on television and radio when multiple studies
6 revealed that “attention and receptivity to cigarette advertising is correlated with both
7 current and future use [by minors].”³² Now, over fifty years later, nicotine peddlers have
8 adapted their product and their method by pushing e-cigarettes through data-driven
9 “social media influencers, hashtags, music videos, and other informal social media
10 presence” advertising.³³ As a result, the “United States is seeing an explosive rise of
11 adolescents’ vaping and the renormalization of smoking” driven by a drastic increase in
12 e-cigarette use among high schoolers.”³⁴

13 76. Online child-targeted advertising is a big problem – but without the data
14 collected by companies like Defendants, it would not be nearly as effective.

19 ³¹ Radesky, *supra* note 27.

20 ³² *Id.*

21 ³³ *Id.*

³⁴ Kristen Jones & Gary A Salzman, *The Vaping Epidemic in Adolescents*, 117 MO. MED. 56-58 (Jan. 2020),
available online at: <https://pmc.ncbi.nlm.nih.gov/articles/PMC7023954/>.

1 **iii. Pixels Can Record Almost Every Interaction Between a User and a**
2 **Platform**

3 77. In order to use Google and Microsoft’s Business Tools, Defendants took
4 several affirmative steps to install and configure Google and Microsoft’s Tracking Tools,
5 including tracking Pixels, onto their website.³⁵

6 78. Pixels are one of the tools used by website operators to track user behavior.
7 As the FTC explains, a Pixel is:

8 [A] small piece of code that will be placed into the website or ad and define
9 [the Pixel operator’s] tracking goals such as purchases, clicks, or
10 pageviews...

11 Pixel tracking can be monetized several ways. One way to monetize pixel
12 tracking is for companies to use the tracking data collected to improve the
13 company's own marketing campaigns...Another is that companies can
14 monetize the data collected by further optimizing their own ad targeting
15 systems and charging other companies to use its advertising offerings.³⁶

16 79. Pixels can collect a shocking amount of information regarding an
17 individual’s online behavior, including the webpages viewed by the user, the amount of
18 time spent by the user on specific webpages, the specific buttons and hyperlinks that the
19 user clicks, the items that the user adds to an online shopping cart, the purchases that a
20 user makes through an online retailer, the text entered by the user into a website search

21

³⁵ See [GA4] Set up Analytics for a website and/or app, ANALYTICS HELP, <https://support.google.com/analytics/answer/9304153?hl=en> (last visited Oct. 20, 2025) (process for installing Google Analytics on a website); Setup Clarity, MICROSOFT LEARN (Aug. 13, 2025), <https://learn.microsoft.com/en-us/clarity/setup-and-installation/clarity-setup> (last visited Oct. 20, 2025).
³⁶ *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking*, FEDERAL TRADE COMMISSION – OFFICE OF TECHNOLOGY (Mar. 6, 2023), <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking> (last visited Aug. 1, 2025).

1 bar, and even the information provided by the user on an online form.³⁷ Microsoft's
2 Clarity tool even provides detailed telemetric data showing, *inter alia*, where the user
3 moves their mouse while using a webpage, how far they scroll, and the areas of the
4 webpage they spent the most time reviewing.³⁸

5 80. But most internet users are completely unaware that substantial information
6 about their internet usage is being collected through tracking Pixels. The FTC warns
7 that:

8 Traditional controls such as blocking third party cookies may not entirely
9 prevent pixels from collecting and sharing information. Additionally, many
10 consumers may not realize that tracking pixels exist because they're
11 invisibly embedded within web pages that users might interact
12 with...Academic and public reporting teams have found that thousands of
13 the most visited webpages have pixels and other methods that leak personal
14 information to third parties.³⁹

15 **iv. The Pixels Installed on Defendants' Platform Transmit Personally
16 Identifiable Information to Google and Microsoft**

17 81. Every website is hosted by a computer "server" that holds the website's
18 contents.

19 82. To access a website, individuals use "web browsers." Web browsers are
20 software applications that allow consumers to navigate the web and view and exchange
21

³⁷ See *id.*; *How does retargeting on Facebook help your business?*, META, <https://www.facebook.com/business/goals/retargeting> (last visited Aug. 1, 2025); Tom Kemp, "Oops! I Did It Again" ... Meta Pixel Still Hoovering Up Our Sensitive Data, MEDIUM, https://tomkemp00.medium.com/oops-i-did-it-again-meta-pixel-still-hoovering-up-our-sensitive-data-f99c7b779d47#_ftn1 (last visited Aug. 1, 2025).

³⁸ *Heatmaps*, MICROSOFT, <https://clarity.microsoft.com/> (last visited Aug. 1, 2025).

³⁹ *Lurking Beneath the Surface*, *supra* note 36.

1 electronic information and communications over the Internet. Each “client device”
2 (such as a computer, tablet, or smartphone) accesses web content through a web browser
3 (such as Google’s Chrome, Mozilla’s Firefox, Apple’s Safari, or Microsoft’s Edge).

4 83. Communications between a website server and web browser consist of
5 Requests and Responses. Any given browsing session may consist of hundreds or even
6 thousands of individual Requests and Responses. A web browser’s Request essentially
7 asks the website to provide certain information, such as the contents of a given webpage
8 when the user clicks a link, and the Response from the website sends back the requested
9 information – the web pages’ images, words, buttons, and other features that the browser
10 shows on the user’s screen as they navigate the website.

11 84. Additionally, on most websites, the Response sent back to the user’s web
12 browser directs the browser to create small files known as ‘cookies’ on the user’s
13 device.⁴⁰ These cookies are saved by the user’s web browser, and are used to identify the
14 website user and information about them as they browse the website or on subsequent
15 visits to the site.⁴¹ For example, in a more innocuous use case, a cookie may allow the
16 website to remember a user’s name and password, language settings, or shopping cart
17 contents.⁴²

19 _____
20 ⁴⁰ *What is a web browser?*, MOZILLA, <https://www.mozilla.org/en-US/firefox/browsers/what-is-a-browser/> (last
visited Aug. 1, 2025).

21 ⁴¹ *Id.*

⁴² *Id.*

1 85. When a Google and/or Microsoft user logs onto their account, their web
2 browser records a Google and/or Microsoft tracking cookie.⁴³ These cookies include a
3 specific line of code that links the web browser to the user’s Google and/or Microsoft
4 account.⁴⁴ With regards to Microsoft, this information is even linked to the individual’s
5 LinkedIn profile, which contains significant identifying information including the
6 individual’s name, location, contact information, educational background, and work
7 history.⁴⁵

8 86. Google and Microsoft’s Pixels use cookies, but operate differently than
9 cookies. Rather than directing the browser to save a file on the user’s device, a Pixel
10 surreptitiously acquires information from the browser, without notifying the user. The
11 information can include details about the user, his or her interactions with the Platform,
12 and information about the user’s environment (*e.g.*, type of device, type of browser, and
13 sometimes even the physical location of the device).

14 87. Simultaneously, the Google and Microsoft Pixels, like those installed on
15 Defendants’ Platform, request identifying information from any Google and Microsoft
16 cookies previously installed on the user’s web browser.

19 ⁴³ Cyphers, *supra* note 21.

20 ⁴⁴ *Id.*

21 ⁴⁵ Mallory Harwood, *Reach specific audiences with LinkedIn Profile Targeting*, MICROSOFT ADVERTISING BLOG (Mar. 9, 2022), <https://about.ads.microsoft.com/en/blog/post/march-2022/reach-specific-audiences-with-linkedin-profile-targeting> (last visited Aug. 1, 2025).

1 88. The Pixel then combines the data it received from the browser with the data
2 it acquired from the cookie, and instructs the web browser to transmit the information
3 back to Google and Microsoft. As a result, Google and Microsoft can link all of the user
4 information collected by their Pixels on the Defendants' Platform to the user's identity,
5 via the user's Google or Microsoft profile. Thus, even if a user never actually logs into
6 a website, or fills out a form, they can still be identified by the Tracking Tools.

7 89. A remarkable number of Americans possess a Google or Microsoft account.
8 Approximately 230 million Americans use Microsoft's Windows operating system,⁴⁶
9 and 230-million Americans are members of Microsoft's LinkedIn social network.⁴⁷ One-
10 third of Americans have accounts with Google's Gmail e-mail client, and over 80-
11 percent of Americans use YouTube, Google's video client.⁴⁸ When these users visit a
12 web service, like Defendants', that utilizes a Google or Microsoft Pixel, any information
13 collected by the Pixel can be linked to the user's identity through the Google and
14 Microsoft cookies installed on the user's web browser.

17 ⁴⁶ Medhi Rizvi, *How Many People Use Windows Worldwide*, TECH SEARCHERS (Apr. 15, 2025), [How Many People Use Windows Worldwide - Tech Searchers](#) (last visited Oct. 17, 2025).

18 ⁴⁷ Naveen Kumar, *How Many People Use LinkedIn In 2025*, DEMANDSAGE (May 14, 2025), <https://www.demandsage.com/linkedin-statistics/> (last accessed Aug. 27, 2025).

19 ⁴⁸ See Harsha Kiran, *49 Gmail Statistics To Show How Big It Is In 2024*, TECHJURY (Jan. 3, 2024), <https://techjury.net/blog/gmail-statistics/> (last accessed Aug. 27, 2025) ("Gmail accounts for 130.9 million of the total email users in the US"). The United States population is approximately 337.4 million. See UNITED STATES CENSUS BUREAU, <https://www.census.gov/popclock/> (last accessed Aug. 27, 2025); Jeffrey Gottfried, *Americans' Social Media Use*, PEW RESEARCH (Jan. 31, 2024), <https://www.pewresearch.org/internet/2024/01/31/americans-social-media-use/> (last visited Aug. 27, 2025).

1 90. However, it is not only Google and Microsoft account holders that are at
2 risk of having Pixel-collected website data linked to their identities. Rather, Google and
3 Microsoft utilize sophisticated data tracking methods to identify even those few users
4 who do not have a Google or Microsoft account.

5 91. Google and Microsoft’s Pixels, like those on the Platform, can acquire
6 information about the user’s device and browser, such as their screen resolution, time
7 zone setting, browser software type and version, operating system type and version,
8 language setting, and IP address.

9 92. An internet user’s combination of such device and browser characteristics,
10 commonly referred to as their “browser fingerprint,” is “often unique.”⁴⁹ By tracking
11 this browser fingerprint, Google and Microsoft are able to compile a user’s activity
12 across the internet.⁵⁰ Moreover, as Google and Microsoft continuously compile user data
13 over time, their understanding of the user’s browser fingerprint becomes more
14 sophisticated such that they need only to collect a single piece of identifying information
15 to identify the user linked to a browser fingerprint.

16 93. While debating the VPPA on the Senate floor in 1988, Senator Patrick
17 Leahy remarked:

18 [I]n an era of interactive television cables, the growth of computer checking
19 and check-out counters, of security systems and telephones, all lodged
together in computers, it would be relatively easy at some point to give a

20 _____
⁴⁹ Cyphers, *supra* note 21.

21 ⁵⁰ *Id.*

1 profile of a person and tell what they buy in a store, what kind of food they
2 like, what sort of television programs they watch, who are some of the
3 people they telephone...I think that is wrong. I think that really is Big
4 Brother, and I think it is something that we have to guard against...
[Privacy] is not a conservative or a liberal or moderate issue. It is an issue
that goes to the deepest yearnings of all Americans that we are free and we
cherish our freedom and we want our freedom. We want to be left alone.

5 S. Rep. No. 100-599 at pp. 5-6 (1988).

6 94. Now, almost forty years later, Senator Leahy's nightmare has become
7 reality. Through the use of Internet surveillance technology, almost every facet of our
8 relationships, interests, aspirations, and beliefs can be tracked, recorded, and packaged
9 for corporate profit by website operators like Defendants.

10 95. Through this action, Plaintiffs seek to send Defendants, and other
11 corporations like them, the same message that Senator Leahy elucidated during the
12 Internet's infancy: "[W]e are free and we cherish our freedom and we want our freedom.
13 We want to be left alone." *Id.*

14 **v. Defendants Disclosed Plaintiffs' Children's and Class Members'
15 Private Children's Data to Google and Microsoft**

16 96. Defendants' video content can be accessed on the Platform on the Internet
17 or by using Defendants' many mobile, tablet, smart TV, and desktop apps. Plaintiffs'
18 Children all accessed the Platform and viewed Defendants' video content.

19 97. Unbeknownst to Plaintiffs, Plaintiffs' Children, and Class Members,
20 Defendants intentionally configured the Google and Microsoft Pixels installed on the
21 Platform to capture and transmit the Private Children's Data that Plaintiffs' Children and

1 Class Members communicated to Defendants while watching their video content on the
2 Platform to at least two unauthorized parties.

3 98. For example, the following screenshots (“Figures 1 & 2”) depicts network
4 transmission data captured while an Internet user watches a video on the “Kids” section
5 of the Platform. Figures 1 & 2 show that when Platform visitors, like Plaintiffs’ Children
6 and Class Members, view Defendants’ video content, the information requested and
7 transmitted to Google and Microsoft by the Tracking Tools installed on Defendant’s
8 website include the title of the video, and the URL at which the video is located.

9 99. Further, the information transmitted to Google and Microsoft is
10 accompanied by specific lines of code linking the information to the user’s identity.

11 100. Figure 1 depicts network transmissions made to Microsoft from the Kids
12 section of the Platform. As Figure 1 shows, alongside the title of the video (in this
13 example, “Rugrats Go Wild”) and its URL, Defendants’ Platform transmitted the
14 identifier number attached to the user’s “MUID” cookie which identifies the user’s
15 Microsoft account. Additionally, the list of bracketed number coordinates in Figure 1
16 encode detailed telemetric data recorded by the Tracking Tool showing, *inter alia*, where
17 the user moved their mouse, how far they scrolled, and the areas of the webpage that the
18 user spent the most time reviewing. Defendants’ Platform also transmitted information
19 that is commonly used to create a browser fingerprint, such as the user’s IP address,
20
21

1 language selection, screen resolution, microprocessor type, internet browser software
2 and version number, and operating system software and version number.

3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21

```

POST https://i.clarity.ms/collect HTTP/1.1
Host: i.clarity.ms
Connection: keep-alive
Content-Length: 5810
sec-ch-ua-platform: "Windows"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
sec-ch-ua: "(Not)A;Brand";v="8", "Chromium";v="138", "Google Chrome";v="138"
Content-Type: text/plain;charset=UTF-8
sec-ch-ua-mobile: ?0
Accept: */*
Origin: https://pluto.tv
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: empty
Sec-Fetch-Storage-Access: active
Referer: https://pluto.tv/
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.9
Cookie: MUID=2931C5CC117164B511B2D3D710CF6587

{"a":["0.8.19",4,6622,1649,"9mlh9nu2wz","j3xank","eikr1l",6,1,1,0,"https://pluto.tv/us/on-demand/movies/61c2323f68b5ad001a6211e1/details"],"a":[[1197,12,680,68,961],[1219,12,680,72,959],[1227,12,680,73,958],[1257,12,636,88,952],[1267,12,636,91,951],[1272,12,597,100,948],[1279,12,408,110,945],[1287,12,408,121,942],[1318,12,596,147,932],[1324,12,596,154,925],[1332,12,596,163,917],[1339,12,596,176,901],[1347,12,408,185,891],[1377,12,4647,282,801],[1386,12,4647,305,783],[1422,12,4647,387,725],[1444,12,4647,401,713],[1489,12,5163,412,694],[1805,12,5163,412,695],[1842,12,5163,412,693],[1857,12,5163,412,692],[1880,12,5163,412,690],[1902,12,5163,412,687],[1910,12,5163,412,684],[1917,12,5162,413,681],[1924,12,4620,416,672],[1932,12,4620,420,661],[1939,12,4563,423,649],[1947,12,4563,427,637],[1954,12,4980,430,623],[1962,12,4980,434,613],[1969,12,4980,438,601],[1977,12,4980,444,580],[1984,12,4980,446,569],[1992,12,4980,448,546],[1999,12,4980,451,531],[2007,12,4980,452,519],[2014,12,4980,453,499],[2024,12,4980,454,489],[2029,12,4980,454,475],[2044,12,4980,455,457],[2068,12,4980,456,447],[2090,12,4980,458,437],[2105,12,4980,458,433],[2119,12,4980,458,432],[2269,15,4980,458,432],[2307,15,4980,458,432],[2344,15,4980,458,432],[2352,15,4980,458,432],[2374,15,4980,458,431],[2389,15,4980,456,430],[2397,12,548,455,429],[2415,12,548,453,428],[2434,12,548,446,419],[2443,12,548,442,413],[2465,12,548,436,403],[2472,12,548,434,399],[2488,12,548,423,375],[2495,12,548,415,357],[2502,12,548,410,346],[2510,12,548,403,328],[2517,12,548,399,317],[2539,12,548,384,274],[2547,12,548,380,263],[2562,12,548,374,247],[2584,12,548,368,230],[2607,12,548,364,224],[2659,12,548,363,224],[2674,12,548,359,230],[2682,12,548,354,244],[2691,12,548,351,256],[2697,12,548,348,270],[2719,12,5319,338,319],[2727,12,5319,334,331],[2734,12,5288,332,343],[2749,12,5288,329,352],[2757,12,4882,328,358],[2764,12,4885,327,360],[2787,12,4885,326,371],[2810,12,4885,326,375],[2869,12,4885,327,375],[2884,12,4885,330,380],[2893,12,4882,332,382],[2899,12,4935,334,387],[2923,12,4935,341,399],[2944,12,4935,348,414],[2967,12,4935,354,432],[2989,12,4935,359,443],[3004,12,4935,362,451],[3012,12,4935,362,455],[3028,12,548,363,460],[3049,12,548,364,463],[3072,15,4935,364,463],[3259,15,4935,364,463],[3499,15,4935,364,463],[3508,12,548,364,464],[3516,12,548,365,464],[3537,12,548,366,466],[3559,12,548,368,468],[3710,12,548,369,468],[3740,12,548,370,468],[3784,12,548,371,468],[3859,12,4935,372,468],[3913,12,4935,373,468],[3919,15,4935,373,468],[3957,15,4935,373,468],[3979,15,4935,374,469],[4002,12,548,374,470],[4024,12,548,374,472],[4070,12,548,375,473],[4107,12,548,376,474],[4129,12,548,377,475],[4137,12,548,378,475],[4159,12,548,378,476],[4183,12,548,380,479],[4204,12,548,384,487],[4228,12,548,390,499],[4249,12,548,393,511],[4272,12,548,396,529],[4288,12,5049,396,539],[4295,12,4451,396,544],[4309,12,4451,398,554],[4332,12,4451,398,557],[4347,12,4451,398,561],[4363,12,4450,398,562],[4377,12,4450,398,563],[4444,12,4504,398,564],[4452,12,4504,398,565],[4474,12,4504,398,567],[4498,12,4504,399,570],[4519,12,4504,400,579],[4542,12,4504,401,588],[4564,12,4504,404,603],[4572,12,4505,405,605],[4587,12,4505,408,618],[4594,12,4505,410,625],[4602,12,4504,412,631],[4617,12,4504,415,640],[4624,12,4511,417,645],[4640,12,4512,423,657],[4647,12,4512,427,663],[4654,12,4511,430,669],[4663,12,5124,435,678],[4685,12,5124,445,695],[4707,12,5124,455,710],[4729,12,5124,463,723],[4753,12,5124,472,732],[4774,12,5124,477,738],[4797,12,5124,485,745],[4812,12,5124,490,748],[4834,12,5124,496,749],[4857,12,5124,501,749],[4879,12,5124,506,749],[4887,12,5124,507,749],[5045,12,5124,508,749],[5067,12,5124,526,757],[5082,12,5124,545,763],[5098,12,5124,552,767],[5120,12,5124,553,768],[5143,12,5124,556,769],[5158,12,5124,558,771],[5172,12,5124,559,771],[5187,12,5124,560,772],[5210,12,5124,562,773],[5232,12,5124,564,775],[5239,12,5124,564,776],[5247,12,5123,566,777],[5269,12,4521,567,777],[5284,12,4521,570,779],[5292,12,5126,570,780],[5313,12,5126,572,781],[5322,12,5127,573,781],[5344,12,5127,576,783],[5367,12,5127,582,784],[5389,12,5127,591,787],[5412,12,5127,600,789],[5434,12,5127,610,791],[5457,12,5127,615,792],[5479,12,5127,620,793],[5502,12,5127,624,794],[5509,12,5127,626,795],[5539,12,5127,627,795],[5555,12,5127,628,795],[5577,12,5127,630,795],[5584,12,5127,630,796],[5629,12,5127,631,796],[5644,12,5127,632,797],[5674,12,5127,633,797],[5689,12,5127,634,797],[5718,12,5127,635,797],[5727,12,5127,636,797],[5802,12,5127,633,797],[5824,12,5127,627,797],[5847,12,5127,620,797],[5869,12,5127,609,796],[5884,12,5127,592,793],[5907,12,5127,575,797],[5914,12,5123,566,799],[5922,12,5124,562,800],[5944,12,5124,544,803],[5967,12,5124,538,803],[5989,12,5124,537,803],[5997,12,5124,536,803],[6027,12,5124,534,804],[6049,12,5124,531,804],[6073,12,5124,526,800],[6094,12,5124,522,796],[6117,12,5124,518,787],[6140,12,5124,516,777],[6162,12,5124,514,774],[6169,12,5124,514,773],[6192,12,5124,514,772],[6214,12,5124,512,770],[6237,12,5124,511,768],[6244,12,5124,511,767],[6268,12,5124,510,766],[6275,12,5124,510,765],[6304,12,5124,510,764],[6343,12,5124,509,764],[6349,12,5124,509,763],[6373,12,5124,508,763],[6402,12,5124,508,762],[6439,12,5124,508,761],[6462,12,5124,506,759],[6484,12,5124,503,754],[6507,12,5124,500,749],[6529,12,5124,498,743],[6552,12,5124,496,740],[6574,12,5124,494,737],[6597,12,5124,493,734],[6612,12,5124,492,733],[7002,12,5124,492,732],[7024,12,5124,492,731],[7212,12,5124,493,731],[8224,9,5124,493,731,16722,9338,0,1,0,"Rugrats Go Wild"],"https://pluto.tv/on-demand/movies/61c2323f68b5ad001a6211e1/details","7f1p8xqxf.4r9h7by4u",1,1],[6622,4,1,1008,1305,1008,1305,0,86846,67,961,6608,4112,3401,67,961,3317,67,961,3281,67,961,3401,67,961,3401],[8271,0,2,595,3,2,4,6,5,7,7,1,25,244],[8271,36,6,7142,0,7674,0,7999,89,8159,51]]}

```

Figure 1: Screenshot depicting back-end network traffic from Defendants' Platform which shows information transmitted to Microsoft when users watch a video on the Platform.

1 101. Figure 2 depicts network transmissions made to Google from the Platform.
 2 As Figure 2 shows, alongside the URL of the video content, Defendants' Platform
 3 transmitted the identifier number attached to the Google's 'gjid' and 'cid' cookies, which
 4 identify the user's Google account. Defendants' Platform also transmitted information
 5 that is commonly used to create a browser fingerprint, such as the user's IP address,
 6 language selection, screen resolution, microprocessor type, internet browser software
 7 and version number, and operating system software and version number.

v	1
_v	j101
a	964435033
t	pageview
_s	1
dl	https://pluto.tv/us/live-tv/673247127d5da5000817b4d6
dr	https://www.google.com/
ul	en-us
de	UTF-8
dt	Pluto TV - Drop in. Watch Free.
sd	24-bit
sr	2560x1441
vp	1008x1305
je	0
_u	YEBAAAABAAAAACAC~
jid	1978696658
gjid	1358294584
cid	988431445.1753108089
tid	UA-46240460-51
_gid	792295453.1753108089
_r	1
_slc	1
gtm	45He57g1n81NKZQ5T9v835229433za200
gcs	G111
gcd	13r3r3r3r511
dma	0
tag_exp	101509157~103116026~103200004~103233427~104684208~104684211
z	853348521

8
9
10
11
12
13
14
15
16
17
18
19
20 *Figure 2: Screenshot depicting back-end network traffic from Defendants' Platform which shows information transmitted to Google when users watch a video on the Platform.*

1 102. Defendants’ disclosure of the user’s browsing information is not limited
2 solely to their use of Defendants’ video content. Indeed, any interaction on any page of
3 the Platform is recorded and contemporaneously disclosed to Google and Microsoft in
4 the same manner as depicted in Figures 1 and 2.

5 103. In their default state, Google and Microsoft’s Pixels record and transmit
6 only “automatic events,” consisting largely of routine user behavior, such as clicking a
7 link, clicking on an advertisement, or viewing a webpage.⁵¹ Defendants purposely
8 configured the Google and Microsoft Pixels on the Platform to collect and transmit
9 additional user data, including information specifically identifying the videos that the
10 users watch.

11 104. By installing third-party Tracking Tools, including tracking Pixels, on the
12 Platform, and by further configuring those Tracking Tools to collect the user’s Private
13 Children’s Data, Defendants knowingly and intentionally caused Plaintiffs’ Children’s
14 and Class Members’ Private Children’s Data to be transmitted to third parties, including
15 Google and Microsoft.

16
17
18
19
20 ⁵¹ *Automatically Collected Events*, GOOGLE ANALYTICS HELP,
<https://support.google.com/analytics/answer/9234069>, (last visited on Aug. 1, 2025); *About automatic events*,
Google Marketing Platform – *Features*, GOOGLE,
21 <https://marketingplatform.google.com/about/analytics/features/> (last visited Aug. 1, 2025).

1 **D. DEFENDANTS DISCLOSED PLAINTIFFS’ CHILDREN’S AND CLASS**
2 **MEMBERS’ SENSITIVE INFORMATION TO THIRD PARTIES**
3 **WITHOUT OBTAINING INFORMED CONSENT**

4 **vi. Defendants failed to inform Plaintiffs, Plaintiffs’ Children, and Class**
5 **Members of its disclosure of the Private Children’s Data, in violation**
6 **of its Privacy Policy.**

7 105. Defendants admit that “some of [their] services are directed to children”
8 and claim to “recognize the need to provide further privacy protections when it comes
9 to children.”⁵² Moreover, through their Children’s Privacy Policy, Defendants represent
10 that they “will obtain parental consent prior to the collection of [children’s] Personal
11 Information.”⁵³

12 106. Defendants did not abide by these principles and promises. In reality,
13 Defendants collect personally identifying information from minor users of the Platform
14 without obtaining parental consent, and simultaneously share that information with third
15 parties, including Google and Microsoft, in exchange for compensation in the form of
16 advertising, analytics, and marketing services. Then, that data is subsequently used to
17 make data profiles for advertising purposes.

18 107. Defendants breached Plaintiffs’ Children’s and Class Members’ right to
19 privacy by unlawfully disclosing their Private Children’s Data to third parties, including
20 Google and Microsoft. Defendants did not inform Plaintiffs or Plaintiffs’ Children that

21 _____
⁵² *Children’s Privacy Policy*, PARAMOUNT, <https://privacy.paramount.com/en/childrens?r=pluto.tv> (last visited on Aug. 1, 2025).

⁵³ *Id.*

1 it was sharing Plaintiffs' Children's Private Children's Data with third parties, including
2 Google and Microsoft.

3 108. Google and Microsoft guide and caution website operators of the dangers
4 of using their Business Tools without first providing notice of and then obtaining valid
5 consent for invasively collecting protected data.⁵⁴

6 109. By engaging in this improper sharing of information without Plaintiffs' and
7 Class Members' consent, Defendants breached their own Privacy Policy, violated
8 Plaintiffs' Children's and Class Members' right to privacy, and unlawfully disclosed the
9 Private Children's Data.

10 110. Despite never telling Plaintiffs, Plaintiffs' Children, or Class Members,
11 Defendants allowed third parties such as Google and Microsoft to intercept Plaintiffs'
12 and Class Members' Private Children's Data and use it for advertising purposes.

13 **vii. The Tracking Tools Used by Defendants Were Imperceptible to**
14 **Plaintiffs, Plaintiffs' Children, and Class Members.**

15 111. The Tracking Tools installed on the Platform were invisible to Plaintiffs,
16 Plaintiffs' Children, and Class Members. Without analyzing the network information

17 ⁵⁴ See, e.g., *Google Analytics Terms of Service*, GOOGLE MARKETING PLATFORM,
18 <https://marketingplatform.google.com/about/analytics/terms/us/> (last visited Oct. 20, 2025) (“You will not . . . pass
information, hashed or otherwise, to Google that Google could use or recognize as personally identifiable information . . .
.”); *Best practices to avoid sending Personally Identifiable Information (PII)*, ANALYTICS HELP,
19 https://support.google.com/analytics/answer/6366371?hl=en&ref_topic=2919631#zippy=%2Cin-this-article (last visited
Oct. 20, 2025) (guiding website owners to configure data redaction to remove personally identifiable information from
transmission); *Microsoft Products and Services Data Protection Addendum*, MICROSOFT, available at: *Privacy & Security*
20 *Terms*, MICROSOFT, <https://www.microsoft.com/licensing/terms/product/PrivacyandSecurityTerms/all> (last visited Oct.
20, 2025) (Website operators using Clarity “must comply with all laws and regulations applicable to its use of [Clarity],
21 including laws related to biometric data, confidentiality of communications, and Data Protection Requirements.”).

1 transmitted by the Platform through examination of its source code or the use of
2 sophisticated web developer tools, there was no way for a user to discover the presence
3 of the Tracking Tools. As a result, typical internet users, such as Plaintiffs, Plaintiffs'
4 Children, and Class Members, were unable to detect the Tracking Tools on Defendants'
5 Platform. This concern is particularly acute considering that Plaintiffs' Children are
6 minors with no particular technical skills or training.

7 112. Plaintiffs, Plaintiffs' Children, and Class Members were shown no
8 disclaimer or warning that the Private Children's Data would be disclosed to any
9 unauthorized third party without express parental consent. To the contrary, as noted
10 above, Defendants promised to not disclose Private Children's Data without the parents'
11 consent, thereby misleading any parent who took the time to review the Privacy Policy
12 to ensure their child's safety

13 113. Plaintiffs, Plaintiffs' Children, and Class Members did not know that the
14 Private Children's Data was being collected and transmitted to an unauthorized third
15 party.

16 114. Because Plaintiffs, Plaintiffs' Children, and Class Members were not aware
17 of the Google and Microsoft Pixels on the Platform, or that the Private Children's Data
18 would be collected and transmitted to Google and Microsoft, Plaintiffs and Class
19 Members could not and did not consent to Defendants' conduct.

1 **E. DEFENDANTS WERE ENRICHED BY THEIR DISCLOSURE OF**
2 **PLAINTIFFS’ CHILDREN’S AND CLASS MEMBERS’ SENSITIVE**
3 **INFORMATION TO THIRD PARTIES**

4 **i. Defendants Received Material Benefits in Exchange for the Private**
5 **Children’s Data**

6 115. As explained, *supra*, users of Google and Microsoft’s Business Tools, like
7 Defendants, receive access to advertising and marketing analytics services in exchange
8 for installing Google and Microsoft’s Tracking Tools on their website.

9 116. Upon information and belief, Defendants, as users of Google and
10 Microsoft’s Business Tools, received compensation in the form of advanced advertising
11 and data analysis services and/or cost-effective marketing on third-party platforms in
12 exchange for allowing Google and Microsoft to collect Plaintiffs’ Children’s and Class
13 Members’ Private Children’s Data.

14 **ii. The Private Children’s Data Had Financial Value**

15 117. Moreover, Plaintiffs’ Children’s and Class Members’ Private Children’s
16 Data had value, and Defendants’ disclosure and interception of that Private Children’s
17 Data harmed Plaintiffs’ Children and the Class.

18 118. According to the annual reports of Facebook, another major online
19 advertisement retailer, the value it derives from user data has continuously risen. “In
20
21

1 2013, the average American’s data was worth about \$19 per year in advertising sales to
2 Facebook, according to its financial statements. In 2020, [it] was worth \$164 per year.”⁵⁵

3 119. Conservative estimates suggest that in 2018, Internet companies earned
4 \$202 per American user from mining and selling data. That figure is only due to keep
5 increasing; estimates for 2022 are as high as \$434 per user, for a total of more than \$200
6 billion industry wide.

7 120. Several companies have products through which they pay consumers for a
8 license to track certain information. Google, Nielsen, UpVoice, HoneyGain, and
9 SavvyConnect are all companies that pay for browsing history information.

10 121. The unauthorized disclosure of Plaintiffs’ Children’s and Class Members’
11 private and Private Children’s Data has diminished the value of that information,
12 resulting in harm including Plaintiffs’ Children and Class Members.

13 **F. PLAINTIFFS’ CHILDREN’S AND CLASS MEMBERS’ REASONABLE**
14 **EXPECTATION OF PRIVACY**

15 122. At all times when Plaintiffs’ Children and Class Members provided their
16 Private Children’s Data to Defendants, Plaintiffs, Plaintiffs’ Children, and Class
17 Members had a reasonable expectation that the information would remain confidential

18
19 _____
20 ⁵⁵ Geoffrey A. Fowler, *There’s no escape from Facebook, even if you don’t use it*, THE WASHINGTON POST (Aug.
21 29, 2021), <https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/> (last visited
Aug. 1, 2025).

1 and that Defendants would not share the Private Children’s Data with third parties for a
2 commercial purpose without obtaining parental consent.

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

7 124. For example, a recent Consumer Reports study shows that 92-percent of
8 Americans believe that internet companies and websites should be required to obtain
9 consent before selling or sharing consumer data, and the same percentage believe those
10 companies and websites should be required to provide consumers with a complete list
11 of the data that is collected about them.⁵⁶

12 125. Moreover, Americans are particularly sensitive about protecting the
13 privacy of children. In a survey conducted jointly by the Center for Digital Democracy
14 and Common Sense Media, 90-percent of parents disagreed with the statement: “It is
15 okay for advertisers to track and keep a record of a child’s behavior online if they give
16 the child free content[,]” and 93-percent of parents agreed that “a federal law that says
17 that online sites and companies need to ask parents’ permission before they collect

18
19
20 ⁵⁶ *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, CONSUMER
21 REPORTS (May 11, 2017), <https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907> (last visited Aug. 1, 2025).

1 personal information from children under age 13” is a “good idea.”⁵⁷ In light of these
2 results, it is perhaps unsurprising that 80-percent of parents of children 13-years-old or
3 younger report worrying about their child’s privacy when using online apps.⁵⁸

4 126. Personal data privacy and obtaining consent to share Private Children’s
5 Data are material to Plaintiffs and Class Members.

6 **V. TOLLING AND ESTOPPEL**

7 127. Any applicable statutes of limitation have been tolled by Defendants’
8 knowing and active concealment of its incorporation of Google and Microsoft’s
9 Tracking Tools into the Platform.

10 128. The Tracking Tools present on the Platform were and are invisible to the
11 average website visitor.

12 129. Through no fault or lack of diligence, Plaintiffs, Plaintiffs’ Children, and
13 Class Members were deceived and could not reasonably discover Defendants’ deception
14 and unlawful conduct.

15 130. Plaintiffs were ignorant of the information essential to pursue Plaintiffs’
16 Children’s claims, without any fault or lack of diligence on their part.

17
18
19

⁵⁷ *Survey on Children and Online Privacy*, CENTER FOR DIGITAL DEMOCRACY & COMMON SENSE MEDIA (2012),
20 available online at: <https://democraticmedia.org/assets/resources/COPPA-Executive-Summary-and-Findings-1635879421.pdf>.

21 ⁵⁸ *Pixalate's Harris Poll Survey Recap: Children's Privacy in Mobile Apps*, PIXALATE (Mar. 1, 2022),
<https://www.pixalate.com/blog/childrens-online-privacy-harris-poll-recap> (last visited Aug. 1, 2025).

1 131. Defendants knew that their Platform incorporated the Tracking Tools and
2 yet failed to disclose to their users (or, where applicable, their user’s parents), that by
3 viewing Defendants’ video content through the Platform, their Private Children’s Data
4 would be disclosed to unauthorized third parties, including Google and Microsoft. To
5 the contrary, by telling their users that they “will obtain parental consent prior to the
6 collection of [Children’s] Personal Information” and further representing a high regard
7 for the privacy of minor users in their Privacy Policy, Defendants misled Plaintiffs into
8 believing that they would not disclose Plaintiffs’ Children’s information.⁵⁹

9 132. Under the circumstances, Defendants were under a duty to disclose the
10 nature, significance, and consequences of their collection and treatment of Private
11 Children’s Data. In fact, Defendants have still not conceded, acknowledged, or
12 otherwise indicated to Plaintiffs, Plaintiffs’ Children, or Class Members that they
13 disclosed or released the Private Children’s Data to unauthorized third parties.
14 Accordingly, Defendants are estopped from relying on any statute of limitations.

15 133. Moreover, all applicable statutes of limitation have also been tolled
16 pursuant to the discovery rule.

17
18
19
20 ⁵⁹ *Children’s Privacy Policy*, PARAMOUNT, <https://privacy.paramount.com/en/childrens?r=pluto.tv> (last visited
21 on Aug. 1, 2025).

1 134. The earliest that Plaintiffs or Class Members, acting with due diligence,
2 could have reasonably discovered Defendants' conduct would have been shortly before
3 the filing of this Complaint.

4 **VI. CLASS ALLEGATIONS**

5 135. This action is brought by the named Plaintiffs, on behalf of the Plaintiffs
6 Children, and a proposed Class of all other persons similarly situated under Federal
7 Rules of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4).

8 136. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

9 **The Nationwide Class**

10 All minors who watched a video on the Defendants' Platform and whose
11 Private Children's Data was disclosed or transmitted to Microsoft, Google, or
any other unauthorized third party.

12 137. In addition to the claims asserted on behalf of the Nationwide Class,
13 Plaintiffs assert claims on behalf of separate California, Illinois, Indiana, and New Jersey
14 Subclasses, which are defined as follows:

15 **California Subclass**

16 All minors residing in California who watched a video on the Defendants'
17 Platform and whose Private Children's Data was disclosed or transmitted to
Microsoft, Google, or any other unauthorized third party.

18 **Illinois Subclass**

19 All minors residing in Illinois who watched a video on the Defendants'
20 Platform and whose Private Children's Data was disclosed or transmitted to
Microsoft, Google, or any other unauthorized third party.

1 **New Jersey Subclass**

2 All minors residing in New Jersey who watched a video on the Defendants’
3 Platform and whose Private Children’s Data was disclosed or transmitted to
4 Microsoft, Google, or any other unauthorized third party.

4 **Indiana Subclass**

5 All minors residing in Indiana who watched a video on the Defendants’
6 Platform and whose Private Children’s Data was disclosed or transmitted to
7 Microsoft, Google, or any other unauthorized third party.

7 138. Excluded from the proposed Classes are any claims for personal injury,
8 wrongful death, or other property damage sustained by the Class; and any Judge
9 conducting any proceeding in this action and members of their immediate families.

10 139. Plaintiffs reserve the right to amend the definitions of the Class or add
11 subclasses if further information and discovery indicate that the definitions of the Class
12 should be narrowed, expanded, or otherwise modified.

13 140. **Numerosity.** The Class is so numerous that the individual joinder of all
14 members is impracticable. Upon information and belief, there are at least 100,000
15 individuals that have been impacted by Defendants’ actions. Moreover, the exact number
16 of those impacted is generally ascertainable by appropriate discovery and is in the
17 exclusive control of Defendants.

18 141. **Commonality.** Common questions of law or fact arising from Defendants’
19 conduct exist as to all members of the Class, which predominate over any questions
20

21

1 affecting only individual Class Members. These common questions include, but are not
2 limited to, the following:

- 3 a) Whether and to what extent Defendants had a duty to protect the
4 Private Children's Data of Plaintiffs' Children and Class
5 Members;
- 6 b) Whether Defendants had duties not to disclose the Private
7 Children's Data of Plaintiffs' Children and Class Members to
8 unauthorized third parties;
- 9 c) Whether Defendants violated their own privacy policy by
10 disclosing the Private Children's Data of Plaintiffs' Children and
11 Class Members to third parties, including Google and Microsoft,
12 without obtaining the parents' consent;
- 13 d) Whether Defendants did and/or could have obtained sufficient
14 consent to permit tracking of Plaintiffs' Children and Class
15 Members.
- 16 e) Whether Defendants adequately, promptly, and accurately
17 informed Plaintiffs, Plaintiffs' Children, and Class Members that
18 the Private Children's Data would be disclosed to third parties;
- 19 f) Whether Defendants violated the law by failing to promptly
20 notify Plaintiffs, Plaintiffs' Children, and Class Members that the
21 Private Children's Data was being disclosed without their
consent;
- g) Whether Defendants adequately addressed and fixed the
practices which permitted the unauthorized disclosure of
Plaintiffs' Children and Class Members' Private Children's Data;
- h) Whether Defendants engaged in unfair, unlawful, or deceptive
practices by failing to keep the Private Children's Data belonging
to Plaintiffs' Children and Class Members free from
unauthorized disclosure;

- 1 i) Whether Defendants violated the statutes asserted as claims in
2 this Complaint;
- 3 j) Whether Plaintiffs' Children, and Class Members are entitled to
4 actual, consequential, and/or nominal damages as a result of
5 Defendants' wrongful conduct;
- 6 k) Whether Defendants knowingly made false representations as to
7 their data security and/or privacy policy practices;
- 8 l) Whether Defendants knowingly omitted material representations
9 with respect to their data security and/or privacy policy practices;
10 and
- 11 m) Whether Plaintiffs' Children, and Class Members are entitled to
12 injunctive relief to redress the imminent and currently ongoing
13 harm faced as a result of the Defendants' disclosure of their
14 Private Children's Data.

15 142. **Typicality.** Plaintiffs' Children's claims are typical of those of other Class
16 Members because their Private Children's Data, like that of every other Class Member,
17 was compromised as a result of Defendants' incorporation and use of the Tracking Tools.

18 143. **Adequacy.** Plaintiffs and Plaintiffs' Children will fairly and adequately
19 represent and protect the interests of the members of the Class in that they have no
20 disabling conflicts of interest that would be antagonistic to those of the other members
21 of the Class. They seek no relief that is antagonistic or adverse to the members of the
Class and the infringement of the rights and the damages they have suffered are typical
of other Class Members. Plaintiffs have also retained counsel experienced in complex
class action litigation and intend to prosecute this action vigorously.

1 144. **Predominance**. Defendants have engaged in a common course of conduct
2 toward Plaintiffs, Plaintiffs' Children, and Class Members in that the Private Children's
3 Data was unlawfully stored and disclosed to unauthorized third parties, including third
4 parties like Google and Microsoft, in the same way. The common issues arising from
5 Defendants' conduct affecting Class Members set out above predominate over any
6 individualized issues. Adjudication of these common issues in a single action has
7 important and desirable advantages of judicial economy.

8 145. **Superiority**. A class action is superior to other available methods for the
9 fair and efficient adjudication of the controversy. Class treatment of common questions
10 of law and fact is superior to multiple individual actions or piecemeal litigation. Absent
11 a class action, most Class Members would likely find that the cost of litigating their
12 individual claim is prohibitively high and would therefore have no effective remedy. The
13 prosecution of separate actions by individual Class Members would create a risk of
14 inconsistent or varying adjudications with respect to individual Class Members, which
15 would establish incompatible standards of conduct for Defendants. In contrast, the
16 conduct of this action as a class action presents far fewer management difficulties,
17 conserves judicial resources and the parties' resources, and protects the rights of each
18 Class Member.

1 146. Defendants acted on grounds that apply generally to the Class as a whole
2 so that class certification, injunctive relief, and corresponding declaratory relief are
3 appropriate on a class-wide basis.

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

- 8 a) Whether Defendants owed a legal duty to Plaintiffs' Children and
9 the Class to exercise due care in collecting, storing, and
10 safeguarding the Private Children's Data and not disclosing it to
11 unauthorized third parties;
- 12 b) Whether Defendants breached a legal duty to Plaintiffs' Children
13 and the Class to exercise due care in collecting, storing, using,
14 and safeguarding the Private Children's Data;
- 15 c) Whether Defendants failed to comply with their own policies and
16 applicable laws, regulations, and industry standards relating to
17 data security;
- 18 d) Whether Defendants adequately and accurately informed
19 Plaintiffs, Plaintiffs' Children, and Class Members that the
20 Private Children's Data would be disclosed to third parties;
- 21 e) Whether Defendants failed to implement and maintain reasonable
security procedures and practices appropriate to the nature and
scope of the information disclosed to third parties; and
- f) Whether Class Members are entitled to actual, consequential,
and/or nominal damages and/or injunctive relief as a result of
Defendants' wrongful conduct.

1 148. Finally, all members of the proposed Class are readily ascertainable.
2 Defendants have access to identifying information for the Class Members’ affected by
3 the unauthorized disclosures described in this Complaint.

4 **COUNT I**
5 **VIOLATIONS OF THE VIDEO PRIVACY PROTECTION ACT**
6 **18 U.S.C. § 2710, et seq.**
7 **(On Behalf of Plaintiffs’ Children and the Nationwide Class)**

8 149. Plaintiffs repeat and reallege the allegations contained in paragraphs 1
9 through 148 as if fully set forth herein.

10 150. The VPPA provides that “a video tape service provider who knowingly
11 discloses, to any person, personally identifiable information concerning any consumer
12 shall be liable to the aggrieved person[.]” 18 U.S.C. § 2710(b)(1).

13 151. “Personally-identifiable information” is defined to include “information
14 which identifies a person as having requested or obtained specific video materials or
15 services from a video tape service provider.” 18 U.S.C. § 2710(a)(3).

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

19 153. Defendants are both a “video tape service provider” because their primary
20 business is the production, hosting, and streaming of thousands of videos on the Platform
21 (as well as through other mediums), thereby “engag[ing] in the business, in or affecting

1 interstate or foreign commerce, of rental, sale, or delivery of pre-recorded video cassette
2 tapes or similar audio visual materials.” 18 U.S.C. § 2710(a)(4).

3 154. Defendants violated the VPPA by knowingly disclosing Plaintiffs’
4 Children’s and Class Members’ personally identifiable information to Google and
5 Microsoft through the Tracking Tools without obtaining informed, written consent.

6 155. As a result of Defendants’ violation of the VPPA, Plaintiffs, Plaintiffs’
7 Children, and the Class are entitled to all damages available under the VPPA including
8 declaratory relief, injunctive and equitable relief, statutory damages of \$2,500 for each
9 violation of the VPPA, and attorney’s fees, filing fees, and costs.

10 **COUNT II**
11 **COMMON LAW INVASION OF PRIVACY**
12 **(On Behalf of Plaintiffs’ Children and the Nationwide Class and, alternatively,**
13 **the California, Illinois, New Jersey, and Indiana Subclasses)**

14 156. Plaintiffs repeat and reallege the allegations contained in paragraphs 1
15 through 155 as if fully set forth herein.

16 157. Plaintiffs, Plaintiffs’ Children, and Class Members have an interest in: (1)
17 precluding the dissemination and/or misuse of their, or their children’s, Private
18 Children’s Data; and (2) making personal decisions and/or conducting personal
19 activities without observation, intrusion or interference, including, but not limited to, the
20 right to visit and interact with various internet sites without being subjected to the
21 exfiltration of their communications without Plaintiffs’ and Class Members’ knowledge
or consent.

1 158. Plaintiffs' Children and Class Members had a reasonable expectation of
2 privacy in their communications with Defendants via the Platform and the
3 communications platforms and services therein.

4 159. Plaintiffs' Children and Class Members communicated Private Children's
5 Data that they intended for only Defendants to receive and that they understood
6 Defendants would keep private and secure.

7 160. Defendants' disclosure of the substance and nature of those
8 communications to third parties without the knowledge and informed consent of
9 Plaintiffs, Plaintiffs' Children, and Class Members is an intentional intrusion on
10 Plaintiffs' Children's and Class Members' solitude or seclusion.

11 161. Plaintiffs, Plaintiffs' Children, and Class Members had a reasonable
12 expectation of privacy given Defendants' Privacy Policy and other representations.

13 162. Moreover, Plaintiffs, Plaintiffs' Children, and Class Members have a
14 general expectation that the communications at issue in this Complaint, including those
15 relating to and identifying Plaintiffs' Children, would be protected from surreptitious
16 disclosure to third parties.

17 163. Defendants' disclosure of Plaintiffs' Children's and Class Members'
18 Private Children's Data coupled with individually identifying information is highly
19 offensive to the reasonable person.

20 164. As a result of Defendants' actions, Plaintiffs' Children and Class Members
21

1 have suffered harm and injury including, but not limited to, an invasion of their privacy
2 rights.

3 165. Plaintiffs' Children and Class Members have been damaged as a direct and
4 proximate result of Defendants' invasion of their privacy and are entitled to
5 compensatory and/or nominal damages.

6 166. Plaintiffs, Plaintiffs' Children, and Class Members seek appropriate relief
7 for such injury including, but not limited to, damages that will reasonably compensate
8 them for the harm to their privacy interests as a result of the intrusions upon Plaintiffs'
9 Children's and Class Members' privacy.

10 167. Plaintiffs, Plaintiffs' Children, and Class Members are also entitled to
11 punitive damages resulting from the malicious, willful and intentional nature of
12 Defendants' actions, directed at injuring Plaintiffs, Plaintiffs' Children, and Class
13 Members in conscious disregard of their rights. Such damages are needed to deter
14 Defendants from engaging in such conduct in the future.

15 168. Plaintiffs also seek such other relief as the Court may deem just and proper.

16 **COUNT III**
17 **VIOLATIONS OF THE ELECTRONIC COMMUNICATIONS PRIVACY**
18 **ACT ("ECPA"), 18 U.S.C. § 2511(1), et seq.**
19 **Unauthorized Interception, Use, and Disclosure**
20 **(On Behalf of Plaintiffs' Children and the Nationwide Class and, alternatively,**
21 **the California, Illinois, New Jersey, and Indiana Subclasses)**

169. Plaintiffs repeat and reallege the allegations contained in the paragraphs 1
through 168 as if fully set forth herein.

1 170. The ECPA protects both sending and receipt of communications.

2 171. 18 U.S.C. § 2520(a) provides a private right of action to any person whose
3 wire or electronic communications are intercepted, disclosed, or intentionally used in
4 violation of Chapter 119.

5 172. The transmissions of Plaintiffs' Children's Private Children's Data to
6 Defendants' Platform qualify as "communications" under the ECPA's definition of 18
7 U.S.C. § 2510(12).

8 173. Electronic Communications. The transmission of Private Children's Data
9 between Plaintiffs' Children and Class Members and Defendants' Platform with which
10 they chose to exchange communications are "transfer[s] of signs, signals,
11 writing,...data, [and] intelligence of [some] nature transmitted in whole or in part by a
12 wire, radio, electromagnetic, photoelectronic, or photooptical system that affects
13 interstate commerce" and are therefore "electronic communications" within the meaning
14 of 18 U.S.C. § 2510(2).

15 174. Content. The ECPA defines content, when used with respect to electronic
16 communications, to "include[] any information concerning the substance, purport, or
17 meaning of that communication." 18 U.S.C. § 2510(8) (emphasis added).

18 175. Interception. The ECPA defines the interception as the "acquisition of the
19 contents of any wire, electronic, or oral communication through the use of any
20 electronic, mechanical, or other device" and "contents ... include any information
21

1 concerning the substance, purport, or meaning of that communication.” 18 U.S.C. §
2 2510(4), (8).

3 176. Electronical, Mechanical or Other Device. The ECPA defines “electronic,
4 mechanical, or other device” as “any device ... which can be used to intercept a[n] ...
5 electronic communication[.]” 18 U.S.C. § 2510(5). The following constitute “devices”
6 within the meaning of 18 U.S.C. § 2510(5):

- 7 a. Plaintiffs’ Children’s and Class Members’ browsers;
- 8 b. Plaintiffs’ Children’s and Class Members’ computing devices;
- 9 c. Defendants’ web-servers; and
- 10 d. The Pixel code deployed by Defendants to effectuate the sending
11 and acquisition of website user communications.

12 177. By utilizing and embedding the Pixels on the Platform, Defendants
13 intentionally intercepted, endeavored to intercept, and procured another person to
14 intercept, the electronic communications of Plaintiffs’ Children and Class Members, in
15 violation of 18 U.S.C. § 2511(1)(a).

16 178. Specifically, Defendants intercepted Plaintiffs’ Children’s and Class
17 Members’ electronic communications via the Pixels, which tracked, stored, and
18 unlawfully disclosed Plaintiffs’ and Class Members’ Private Information to third parties
19 such as Google and Microsoft.
20
21

1 179. Defendants’ intercepted communications include, but are not limited to,
2 communications to/from Plaintiffs’ Children and Class Members regarding their Private
3 Children’s Data, including the specific videos they viewed on the Platform.

4 180. By intentionally disclosing or endeavoring to disclose the electronic
5 communications of Plaintiffs’ Children and Class Members to third parties, while
6 knowing or having reason to know that the information was obtained through the
7 interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a),
8 Defendants violated 18 U.S.C. § 2511(1)(c).

9 181. By intentionally using, or endeavoring to use, the contents of the electronic
10 communications of Plaintiffs’ Children and Class Members, while knowing or having
11 reason to know that the information was obtained through the interception of an
12 electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendants violated
13 18 U.S.C. § 2511(1)(d).

14 182. Unauthorized Purpose. Defendants intentionally intercepted the contents of
15 Plaintiffs’ Children’s and Class Members’ electronic communications for the purpose of
16 committing a tortious act in violation of the Constitution or the laws of the United States
17 or of any State—namely, invasion of privacy, among others.

18 183. The ECPA provides that a “party to the communication” may be liable
19 where a “communication is intercepted for the purpose of committing any criminal or
20
21

1 tortious act in violation of the Constitution or the laws of the United States or of any
2 State.” 18 U.S.C § 2511(2)(d).

3 184. Defendants are not parties for purposes to the communication based on its
4 unauthorized duplication and transmission of communications with Plaintiffs’ Children
5 and the Class. However, even assuming Defendants are parties, Defendants’
6 simultaneous, unknown duplication, forwarding, and interception of Plaintiffs’
7 Children’s and Class Members’ Private Children’s Data does not qualify for the party
8 exemption.

9 185. Defendants’ acquisition of sensitive communications that were used and
10 disclosed to Google and Microsoft was done for purposes of committing criminal and
11 tortious acts in violation of the laws of the United States and individual States nationwide
12 as set forth herein, including:

- 13 a. Invasion of privacy;
- 14 b. Breach of implied contract;
- 15 c. Violations of VPPA 18 U.S.C. § 2710, *et seq.*;
- 16 d. Violations of the COPPA, 15 U.S.C. 6501, *et seq.*; and
- 17 e. Violations of the California Invasion of Privacy Act (“CIPA”), Cal. Pen.
18 Code § 360, *et seq.*

19 186. Defendants’ conduct violated 42 U.S.C. § 1320d-6 in that it used and caused
20 to be used cookie identifiers associated with specific users, including Plaintiffs’ Children
21

1 and Class Members, without user authorization; and disclosed individually identifiable
2 Private Children's Data to Google and Microsoft without authorization.

3 187. Defendants are not exempt from ECPA liability under 18 U.S.C. §
4 2511(2)(d) on the grounds that they were a participant in Plaintiffs' Children's and Class
5 Members' communications about their Private Children's Data on the Platform. They
6 used their participation in these communications to improperly share Plaintiffs'
7 Children's and Class Members' Private Information with Google, Microsoft and third-
8 parties that did not participate in these communications. Plaintiffs, Plaintiffs' Children,
9 and Class Members did not know these third parties were receiving the Private
10 Children's Data, and Plaintiffs, Plaintiffs' Children, and Class Members did not consent
11 to third parties receiving their Private Children's Data.

12 188. As such, Defendants cannot viably claim any exception to ECPA liability.

13 189. Plaintiffs' Children, and Class Members have suffered damages as a direct
14 and proximate result of Defendants' invasion of privacy in that:

- 15 a. Defendants received substantial financial benefits from their use of
16 Plaintiffs' Children's and Class Members' Private Children's Data
17 without providing any value or benefit to Plaintiffs' Children or Class
18 Members;
- 19 b. Defendants received substantial financial benefits from their use of
20 Plaintiffs' Children's and Class Members' Private Children's Data
21 without providing any value or benefit to Plaintiffs, Plaintiffs'
Children or Class Members;
- c. Defendants received substantial, quantifiable value from their use of
Plaintiffs' Children's and Class Members' Private Children's Data,

1 such as understanding how people use the Platform and determining
2 what ads people see on the Platform, without providing any value or
benefit to Plaintiffs, Plaintiffs' Children, or Class Members;

3 d. The diminution in value of Plaintiffs' Children's and Class Members'
4 Private Children's Data and/or the loss of privacy due to Defendants
5 making such Private Children's Data, which Plaintiffs, Plaintiffs'
Children and Class Members intended to remain private, no longer
private.

6 190. Defendants intentionally used the wire or electronic communications to
7 increase its profit margins. Defendants specifically used the Pixels to track and utilize
8 Plaintiffs' Children's and Class Members' Private Children's Data for financial gain.

9 191. Defendants were not acting under color of law to intercept Plaintiffs'
10 Children's and the Class Members' wire or electronic communication.

11 192. Plaintiffs, Plaintiffs' Children, and Class Members did not authorize
12 Defendants to acquire the content of these communications for purposes of invading
13 their privacy via the Tracking Tools.

14 193. Any purported consent that Defendants may claim to have received from
15 Plaintiffs, Plaintiffs' Children, and Class Members was not valid.

16 194. In sending and acquiring the content of Plaintiffs' Children's and Class
17 Members' communications relating to the browsing of Defendants' Platform,
18 Defendants' purpose was tortious, criminal, and designed to violate federal and state
19 legal provisions including a knowing intrusion into a private, place, conversation, or
20 matter that would be highly offensive to a reasonable person.

21

1 195. As a result of Defendants’ violation of the ECPA, Plaintiffs, Plaintiffs’
2 Children, and the Class are entitled to all damages available under 18 U.S.C. § 2520,
3 including statutory damages of whichever is the greater of \$100 a day for each day of
4 violation or \$10,000, equitable or declaratory relief, compensatory and punitive
5 damages, and attorney’s fees and costs.

6 **COUNT IV**
7 **INVASION OF PRIVACY UNDER CALIFORNIA’S CONSTITUTION**
8 **Cal. Const. Art. 1, § 1**
9 **(On Behalf of Minor Plaintiff B.E. and the California Subclass)**

10 196. Minor Plaintiff B.E. repeats and realleges the allegations contained in
11 paragraphs 1 through 195 as if fully set forth herein.

12 197. Article I, section 1 of the California Constitution provides that “[a]ll people
13 are by nature free and independent and have inalienable rights. Among these are
14 enjoying and defending life and liberty, acquiring, possessing, and protecting property,
15 and pursuing and obtaining safety, happiness, and privacy.”

16 198. The right to privacy in California’s constitution creates a private right of
17 action against private and government entities.

18 199. To state a claim for invasion of privacy under the California Constitution,
19 a plaintiff must establish: (1) a legally protected privacy interest; (2) a reasonable
20 expectation of privacy, and (3) an intrusion so serious in nature, scope, and actual or
21 potential impact as to constitute an egregious breach of the social norms.

1 200. Defendant violated Minor Plaintiff B.E.’s and California Subclass
2 Members’ constitutional right to privacy by collecting, storing and disclosing their
3 personal information in which they had a legally protected privacy interest and for which
4 they had a reasonable expectation of privacy, in a manner that was highly offensive to
5 Minor Plaintiff B.E. and California Subclass Members and was an egregious violation
6 of social norms.

7 201. Defendants have intruded upon Minor Plaintiff B.E.’s and California
8 Subclass Members’ legally protected privacy interests, including interests in precluding
9 the dissemination or misuse of their confidential Personal Information.

10 202. Minor Plaintiff B.E. and California Subclass Members had a reasonable
11 expectation of privacy in that: (i) Defendants’ invasion of privacy occurred as a result of
12 Defendants’ security practices, including the collecting, storage, and unauthorized
13 disclosure of minors’ Private Children’s Data; (ii) Neither Minor Plaintiff B.E. and
14 California Subclass Members, nor their parents, consented to or otherwise authorized
15 Defendants to disclose their Sensitive Information; and (iii) Minor Plaintiff B.E. and
16 California Subclass Members could not reasonably expect Defendants would commit
17 acts in violation of privacy protection laws.

18 203. As a direct and proximate result of Defendants’ invasion of their privacy,
19 Minor Plaintiff B.E. and California Subclass Members have been damaged and have
20 suffered actual and concrete injuries.

21

1 204. Minor Plaintiff B.E. and California Subclass Members are entitled to
2 appropriate relief, including damages to compensate them for the harm to their privacy
3 interests, loss of valuable rights and protections, heightened stress, fear, anxiety, risk of
4 future invasions of privacy and the mental and emotional distress and harm to human
5 dignity interests caused by Defendants’ invasions.

6 205. Minor Plaintiff B.E. and California Subclass Members seek appropriate
7 relief for that injury including, but not limited to, damages that will reasonably Minor
8 Plaintiff B.E. and Subclass Members for the harm to their privacy interests, nominal
9 damages, and/or disgorgement of profits made by Defendants as a result of their
10 intrusions upon Minor Plaintiff B.E.’s and Class Members’ privacy.

11 **COUNT V**
12 **VIOLATIONS OF THE CALIFORNIA INVASION OF PRIVACY ACT**
13 **(“CIPA”)**
14 **Cal. Pen. Code § 360, et seq.**
15 **(On Behalf of Minor Plaintiff B.E. and the California Subclass)**

16 206. Minor Plaintiff B.E. repeats and realleges the allegations contained in
17 paragraphs 1 through 205 as if fully set forth herein.

18 207. The California Legislature enacted CIPA in response to “advances in
19 science and technology” that “have led to the development of new devices and
20 techniques for the purpose of eavesdropping upon private communications[,]”
21 recognizing that “the invasion of privacy resulting from the continual and increasing use
of such devices and techniques has created a serious threat to the free exercise of

1 personal liberties and cannot be tolerated in a free and civilized society.” Cal. Pen. Code.
2 § 630.

3 208. Under CIPA, it is unlawful to:

- 4 i. “[W]illfully and *without the consent of all parties to the*
5 *communication*, or in any unauthorized manner, read[], or attempt[]
6 to read, or to learn the contents or meaning of any message, report,
7 or communication while the same is in transit or passing over any
8 wire, line, or cable, or is being sent from, or received at any place
9 within this state;” or
10 ii. “[U]se, or attempt[] to use, in any manner, or for any purpose, or to
11 communicate in any way, any information so obtained[;]” or
12 iii. “[A]id, agree[] with, employ[], or conspire[] with any person or
13 persons to unlawfully do, or permit, or cause to be done any of the
14 acts [prohibited by CIPA.]”

15 Cal. Penal Code § 631(a) (emphasis added).

16 209. At all relevant times, Defendants aided, employed, agreed with, and
17 conspired with Google, Microsoft and likely other third parties, to track and intercept
18 Plaintiffs’ Children’s and Class Members’ internet communications while using the
19 Platform, specifically by installing and configuring the Tracking Tools to permit Google
20 and Microsoft to eavesdrop on and intercept in real-time the content of intercept
21 Plaintiffs’ Children’s and Class Members’ private communications with Defendants.

22 210. The content of those conversations included Private Children’s Data,
23 including the specific videos that Plaintiffs’ Children and Class Members watched on
24 the Platform. Through Defendants’ installation and configuration of the Tracking Tools

1 on the Platform, these communications were intercepted by Google and Microsoft
2 during the communications and without the knowledge, authorization, or consent of
3 Plaintiffs and Class Members.

4 211. Defendants intentionally inserted electronic devices into the Platform that,
5 without the knowledge and consent of Plaintiffs, Plaintiffs' Children, and Class
6 Members, transmitted the substance of their confidential communications with
7 Defendants to third parties.

8 212. Defendants willingly facilitated Google's, Microsoft's, and other third
9 parties' interception and collection of Plaintiffs' Children's and Class Members' Private
10 Children's Data by embedding the Tracking Tools on the Platform, thereby assisting
11 Google's and Microsoft's eavesdropping.

12 213. The following items constitute "machine[s], instrument[s], or
13 contrivance[s]" under the CIPA, and even if they do not, the Tracking Tools fall under
14 the broad catch-all category of "any other manner":

- 15 i. The computer codes and programs Google, Microsoft, and other third
16 parties used to track intercept Plaintiffs' Children's and Class Members'
communications while they were navigating the Platform;
- 17 ii. Plaintiffs' Children's and Class Members' internet browsers;
- 18 iii. Plaintiffs' Children's and Class Members' computing and mobile
19 devices;
- 20 iv. Google and Microsoft's web and ad servers;
- 21

- v. The web and ad servers from which Google, Microsoft, and other third parties tracked and intercepted Plaintiffs' Children's and Class Members' communications while they were using a web browser to access or navigate the Platform;
- vi. The computer codes and programs used by Google, Microsoft, and other third parties to effectuate their tracking and interception of Plaintiffs' Children's and Class Members' communications while they were using a browser to visit the Platform; and

214. As demonstrated hereinabove, Defendants violated CIPA by aiding and permitting third parties, including Google, Microsoft, and their agents, employees, and contractors, to receive Plaintiffs' Children's and Class Members' Private Children's Data in real time, through the Platform, without obtaining parental consent.

215. By disclosing Plaintiffs' Children's and Class Members' Sensitive information, Defendants violated Plaintiffs' Children's and Class Members' statutorily protected right to privacy.

216. As a result of Defendants' violation of the CIPA, Plaintiffs, Plaintiffs' Children, and Class Members are entitled to treble actual damages related to their loss of privacy in an amount to be determined at trial, statutory damages, attorney's fees, litigation costs, injunctive and declaratory relief, and punitive damages.

COUNT VI
NEGLIGENCE
(On Behalf of Plaintiffs' Children and the Nationwide Class and, alternatively, the California, Illinois, New Jersey, and Indiana Subclasses)

217. Plaintiffs repeat and reallege the allegations contained in in paragraphs 1 through 216 as if fully set forth herein.

1 218. Through using Defendants' Platform, Plaintiffs' Children and Class
2 Members provided it with their Private Children's Data.

3 219. By collecting and storing this data, Defendants had a duty of care to use
4 reasonable means to secure and safeguard it from unauthorized disclosure to third
5 parties.

6 220. Defendants negligently failed to take reasonable steps to protect Plaintiffs'
7 Children's and Class Members' Private Children's Data from being disclosed to third
8 parties, without parental consent, including to Google and Microsoft.

9 221. Defendants further negligently omitted to inform Plaintiffs, Plaintiffs'
10 Children, and Class Members that they would use the Private Children's Data for
11 marketing purposes, or that the Private Children's Data would be transmitted to third
12 parties.

13 222. Defendants knew, or reasonably should have known, that Plaintiffs'
14 Children's and Class Members' would not have provided their Private Children's Data
15 to Defendants, had Plaintiffs, Plaintiffs' Children, and Class Members known that
16 Defendants intended to use that information for unlawful purposes.

17 223. Defendants' conduct has caused Plaintiffs' Children and Class Members to
18 suffer damages by having their Private Children's Data accessed, stored, and
19 disseminated without their knowledge or consent (or the knowledge or consent of their
20 parents).

21

1 224. Plaintiffs, Plaintiffs' Children, and Class Members are entitled to
2 compensatory, nominal, and/or punitive damages.

3 225. Defendants' negligent conduct is ongoing, in that it still holds the Private
4 Children's Data of Plaintiffs' Children and Class Members in an unsafe and unsecure
5 manner. Therefore, Plaintiffs, Plaintiffs' Children, and Class Members are also entitled
6 to injunctive relief requiring Defendants to (i) strengthen their data security systems and
7 monitoring procedures; (ii) submit to future annual audits of those systems and
8 monitoring procedures; and (iii) provide adequate credit monitoring to all Class
9 Members.

10 **COUNT VII**
11 **BREACH OF IMPLIED CONTRACT**
12 **(On Behalf of Plaintiffs' Children and the Nationwide Class and, alternatively,**
13 **the California, Illinois, New Jersey, and Indiana Subclasses)**

14 226. Plaintiffs repeat and reallege the allegations contained in paragraphs 1
15 through 225 as if fully set forth herein.

16 227. When Plaintiffs' Children and Class Members provided their Private
17 Children's Data to Defendants in exchange for services, they entered into an implied
18 contract pursuant to which Defendants agreed to safeguard and not disclose their Private
19 Children's Data without consent.

20 228. Plaintiffs' Children and Class Members accepted Defendants' offers and
21 provided their Private Children's Data to Defendants.

22 229. Plaintiffs, Plaintiffs' Children, and Class Members would not have

1 entrusted Defendants with their, or their child's, Private Children's Data in the absence
2 of an implied contract between them and Defendants obligating Defendants to not
3 disclose Private Children's Data without consent.

4 230. Defendants breached these implied contracts by disclosing Plaintiffs'
5 Children's and Class Members' Private Children's Data to third parties like Google and
6 Microsoft.

7 231. As a direct and proximate result of Defendants' breaches of these implied
8 contracts, Plaintiffs' Children and Class Members sustained damages as alleged herein.

9 232. Plaintiffs' Children and Class Members would not have used Defendants'
10 services had they known their Private Children's Data would be disclosed.

11 233. Plaintiffs, Plaintiffs' Children, and Class Members are entitled to
12 compensatory, consequential, and/or nominal damages as a result of Defendants'
13 breaches of implied contract.

14 **COUNT VIII**
15 **UNJUST ENRICHMENT**
16 **(On Behalf of Plaintiffs' Children and the Nationwide Class and, alternatively,**
17 **the California, Illinois, New Jersey, and Indiana Subclasses)**

18 234. Plaintiffs repeat and reallege the allegations contained in paragraphs 1
19 through 233 as if fully set forth herein.

20 235. Plaintiffs plead this claim in the alternative to their breach of implied
21 contract claim.

236. Plaintiffs' Children and Class Members conferred a monetary benefit on

1 Defendants. Specifically, they provided their Private Children’s Data to Defendants,
2 which it exchanged for marketing and advertising services, as described, *supra*.

3 237. Defendants knew that Plaintiffs’ Children and Class Members conferred a
4 benefit which Defendants accepted. Defendants profited from the Private Children’s
5 Data of Plaintiffs’ Children and Class Members by exchanging it for marketing and
6 advertising services.

7 238. In particular, Defendants enriched themselves by obtaining the inherent
8 value of that Plaintiffs’ Children’s and Class Members’ Private Children’s Data, and by
9 saving the costs it reasonably should have expended on marketing and/or data security
10 measures to secure that Minor Plaintiff’s and Class Members’ Private Children’s Data.

11 239. Plaintiffs’ Children and Class Members, on the other hand, suffered as a
12 direct and proximate result of Defendants’ decision to prioritize their own profits over
13 the privacy of their Private Children’s Data.

14 240. Under the principles of equity and good conscience, Defendants should not
15 be permitted to retain the money belonging to Plaintiffs’ Children and Class Members,
16 obtained by their surreptitious collection and transmission of the Private Children’s
17 Data.

18 241. If Plaintiffs, Plaintiffs’ Children, and Class Members knew that Defendants
19 had not reasonably secured their Private Children’s Data, they would not have agreed to
20 provide their, or their child’s, Private Children’s Data to Defendants.

21

1 242. Plaintiffs, Plaintiffs' Children, and Class Members have no adequate
2 remedy at law for this count. An unjust enrichment theory provides the equitable
3 disgorgement of profits even where an individual has not suffered a corresponding loss
4 in the form of money damages.

5 243. As a direct and proximate result of Defendants' conduct, Plaintiffs,
6 Plaintiffs' Children, and Class Members have suffered and will continue to suffer injury.

7 244. Defendants should be compelled to disgorge into a common fund or
8 constructive trust, for the benefit of Plaintiffs, Plaintiffs' Children, and Class Members,
9 proceeds that they unjustly received from them.

10 **PRAYER FOR RELIEF**

11 **WHEREFORE**, Plaintiffs, on behalf of themselves, Plaintiffs' Children, and the
12 putative Class, pray for judgment against Defendants as follows:

- 13 A. an Order certifying the Nationwide Class and California, Illinois,
14 and New Jersey Subclasses, and appointing the Plaintiffs and their
15 Counsel to represent the Classes;
- 16 B. equitable relief enjoining Defendants from engaging in the
17 wrongful conduct complained of herein pertaining to the misuse
18 and/or disclosure of the Private Children's Data of Plaintiffs'
19 Children and Class Members;
- 20 C. injunctive relief requested by Plaintiffs, including, but not limited
21 to, injunctive and other equitable relief as is necessary to protect the
interests of Plaintiffs, Plaintiffs' Children, and Class Members;
- D. an award of all damages available at equity or law, including, but
not limited to, actual, consequential, punitive, statutory and
nominal damages, as allowed by law in an amount to be
determined;

- 1 E. an award of attorney fees, costs, and litigation expenses, as allowed
by law;
- 2 F. prejudgment interest on all amounts awarded and
- 3 G. all such other and further relief as this Court may deem just and proper.

4 **DEMAND FOR JURY TRIAL**

5 Plaintiffs, on behalf of Plaintiffs' Children and other members of the proposed
6 Classes, hereby demand a jury trial on all issues so triable.

7
8 Dated: November 4, 2025

Respectfully submitted,

9 /s/ Daniel Srourian

Daniel Srourian, Esq. (SBN 285678)

10 **SROURIAN LAW FIRM, P.C.**

468 N. Camden Dr. Suite 200

Beverly Hills, CA 90210

11 Telephone: (213) 474-3800

12 Facsimile: (213) 471-4160

Email: daniel@slfla.com

13 Tyler J. Bean*

14 Sonjay C. Singh*

SIRI & GLIMSTAD LLP

745 Fifth Avenue, Suite 500

New York, New York 10151

16 Tel: (212) 532-1091

E: tbean@sirillp.com

17 E: ssingh@sirillp.com

18 **pro hac vice admission anticipated*

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Paramount Lawsuit Claims Pluto TV Harvests Personal Info from Videos Watched by Children](#)
