

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

LISA ADDI, individually and on behalf of all
other persons similarly situated,

Plaintiff,

v.

THE INTERNATIONAL BUSINESS
MACHINES, INC.,

Defendant.

Case No. 7:23-cv-5203-NSR

Hon. Nelson S. Román

**FIRST AMENDED CLASS ACTION
COMPLAINT**

JURY TRIAL DEMANDED

Dated: September 19, 2023

BURSOR & FISHER, P.A.

Joseph I. Marchese
Max S. Roberts
Julian C. Diamond
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-Mail: jmarchese@bursor.com
mroberts@bursor.com
jdiamond@bursor.com

BURSOR & FISHER, P.A.

Christopher R. Reilly*
701 Brickell Ave., Suite 1420
Miami, FL 33131
Telephone: (305) 330-5512
Facsimile: (305) 676-9006
E-Mail: creilly@bursor.com

**Pro Hac Vice forthcoming*

Attorneys for Plaintiff

TABLE OF CONTENTS

	PAGE(S)
NATURE OF THE ACTION	1
PARTIES	2
JURISDICTION AND VENUE	3
STATEMENT OF FACTS	4
I. DEFENDANT IS A VIDEO TAPE SERVICE PROVIDER.....	4
II. DEFENDANT KNOWINGLY DISCLOSES CONSUMERS’ PERSONALLY IDENTIFIABLE INFORMATION TO THIRD PARTIES, AND WILLFULLY PROCURES THIRD PARTIES TO INTERCEPT THE CONTENTS OF WEBSITE COMMUNICATIONS.....	5
A. Testing Reveals That Defendant Illegally Shares Its’ Consumers PII And Video-Viewing Information With Third Parties, And That Third Parties, As Procured By Defendant, Intercept The Contents Of Website Users’ Communications	5
1. Overview Of mParticle.....	7
2. Overview Of AdNexus/Xandr.....	8
B. Defendant Discloses PII To Third Parties, And Third Parties, As Procured By Defendant, Intercept The Content Of Users’ Communications.....	9
1. Defendant Discloses Users’ Names And E-Mail Addresses To Third Parties, And Third Parties Intercept Users’ Names And E-Mail Addresses	10
2. Defendant Discloses Users’ Precise Geolocation To Third Parties, And Third Parties Intercept Users’ Precise Geolocation	11
3. Defendant Discloses Information Identifying Which Specific Videos Were Watched By Which Specific Users, And Third Parties Intercept Information Identifying Which Specific Videos Were Watched By Which Specific Users	13
C. Defendant Discloses Personally Identifiable Information To Third Parties For The Purpose Of Marketing, Advertising, And Website Analytics.....	15

1.	Defendant Discloses Personally Identifiable Information To mParticle, And Defendant Procures mParticle To Intercept The Contents Of Website Communications, For The Purpose Of Marketing, Advertising, And Website Analytics	16
2.	Defendant Discloses Personally Identifiable Information To AdNexus/Xandr, And Defendant Procures mParticle To Intercept The Contents Of Website Communications, For The Purpose Of Marketing, Advertising, And Website Analytics	20
D.	Defendant Knowingly Discloses Its Consumers’ PII To mParticle And AdNexus/Xandr, And Willfully Procures mParticle And AdNexus/Xandr To Intercept The Content Of Website Users’ Communications.....	23
	CLASS ALLEGATIONS	24
	CAUSES OF ACTION.....	26
	Violation Of The VPPA, 18 U.S.C. § 2710.....	26
	Violation Of The Maryland Wiretapping And Electronic Surveillance Act, Md. Code Cts. & Jud. Proc. §§ 10-401, <i>et seq.</i>	29
	Unjust Enrichment.....	32
	PRAYER FOR RELIEF	33
	JURY TRIAL DEMANDED.....	34

Plaintiff Lisa Addi (“Plaintiff”), individually and behalf of all others similarly situated, brings this class action against Defendant The International Business Machines Corporation (“Defendant” or “IBM”). Plaintiff makes the following allegations pursuant to the investigation of her counsel and based upon information and belief, except as to the allegations specifically pertaining to herself, which are based on personal knowledge.

NATURE OF THE ACTION

1. This is a class action suit brought against Defendant The International Business Machines, Inc. (“IBM” or “Defendant”) for violating the Video Privacy Protection Act, 18 U.S.C. § 2710 (“VPPA”), and the Maryland Wiretapping and Electronic Surveillance Act, Md. Code Cts. & Jud. Proc. §§ 10-401, *et seq.* (“MWESCA”).

2. Defendant owns and operates The Weather Channel website, weather.com (the “Website”), which provides pre-recorded video content for weather-related news stories.

3. Unbeknownst to Plaintiff and Class Members, Defendant knowingly and willfully disclosed its users’ personally identifiable information—including a record of every video viewed by the user—to unrelated third parties, mParticle and AdNexus (now known as “Xandr”). By doing so, Defendant violated the VPPA.

4. Further, unbeknownst to Plaintiff and Class Members, Defendant procured third parties, mParticle and AdNexus/Xandr, to secretly observe, record, and otherwise intercept website visitors’ electronic communications with Defendant and use that data to improve their own marketing and analytical capabilities, as well as those of Defendant. By doing so, Defendant violated the MWESCA.

5. During the months of May and June 2023, Plaintiff visited the Website and watched pre-recorded videos after creating an account. During these visits, Defendant transmitted

Plaintiffs' video-viewing information and personally identifying information ("PII") to mParticle and AdNexus/Xandr. Likewise, mParticle and AdNexus/Xandr, as procured by Defendant, recorded and thereby intercepted Plaintiff's electronic communications in real time with Defendant.

6. Plaintiff brings this action for damages and other legal and equitable remedies resulting from Defendant's violations of the VPPA and the MWESCA.

PARTIES

7. Plaintiff Lisa Addi is a resident of Maryland and has an intent to remain there and is therefore a citizen of Maryland. Ms. Addi has long had a Website account and used the Website to watch pre-recorded, weather-related videos. Most recently, in or about May 2023, prior to the filing of this lawsuit, Ms. Addi browsed the Website on her computer and viewed pre-recorded videos on the Website. Ms. Addi was in Maryland when she visited the website, and was logged in to her account.

8. As alleged in more detail below, when Ms. Addi watched a pre-recorded video on the Website, Ms. Addi's full name, gender, e-mail address, precise geolocation, the name of the videos she watched, and the URLs of videos she watched—which listed the name of the video—were disclosed by Defendant to third parties, mParticle and AdNexus/Xandr.

9. Likewise, when Ms. Addi watched a pre-recorded video on the Website, Ms. Addi's full name, gender, e-mail address, precise geolocation, the name of the videos she watched, and the URLs of videos she watched—which listed the name of the video—were intercepted in real time by mParticle and AdNexus/Xandr, as procured by Defendant.

10. Using the information they acquired through the disclosure and interception of Ms. Addi's user data, mParticle and AdNexus/Xandr were able to analyze and track Ms. Addi's activity

across the Website, target Ms. Addi with relevant advertising, and assist Defendant with revenue generation by factoring Ms. Addi's user data into a real-time bidding process.

11. At all times relevant, Ms. Addi was unaware at the time that her full name, gender, e-mail, precise geolocation, names of videos watched, and URLs of videos watched were being sent to and intercepted in real-time by mParticle and AdNexus/Xandr, nor did Ms. Addi consent to the same.

12. Ms. Addi never consented, agreed, nor otherwise permitted Defendant to disclose her personally identifying information to third parties, or procure third parties to intercept her personally identifying information, and certainly did not do so for purposes violative of the VPPA and MWESCA.

13. Likewise, Defendant never gave Ms. Addi the opportunity to prevent the disclosure to and interception of her PII by third parties.

14. Defendant IBM is a New York company with its principal place of business at 1 New Orchard Road, Armonk, NY 10504. IBM owns and operates Weather.com.

JURISDICTION AND VENUE

15. The Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331 because the VPPA is a federal statute.

16. This Court also has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of \$5,000,000.00, exclusive of interest and costs, and at least one member of the proposed class is citizen of state different from at least one Defendant.

17. This Court has general personal jurisdiction over Defendant because Defendant maintains its principal place of business in New York.

18. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) because Defendant resides in this District.

STATEMENT OF FACTS

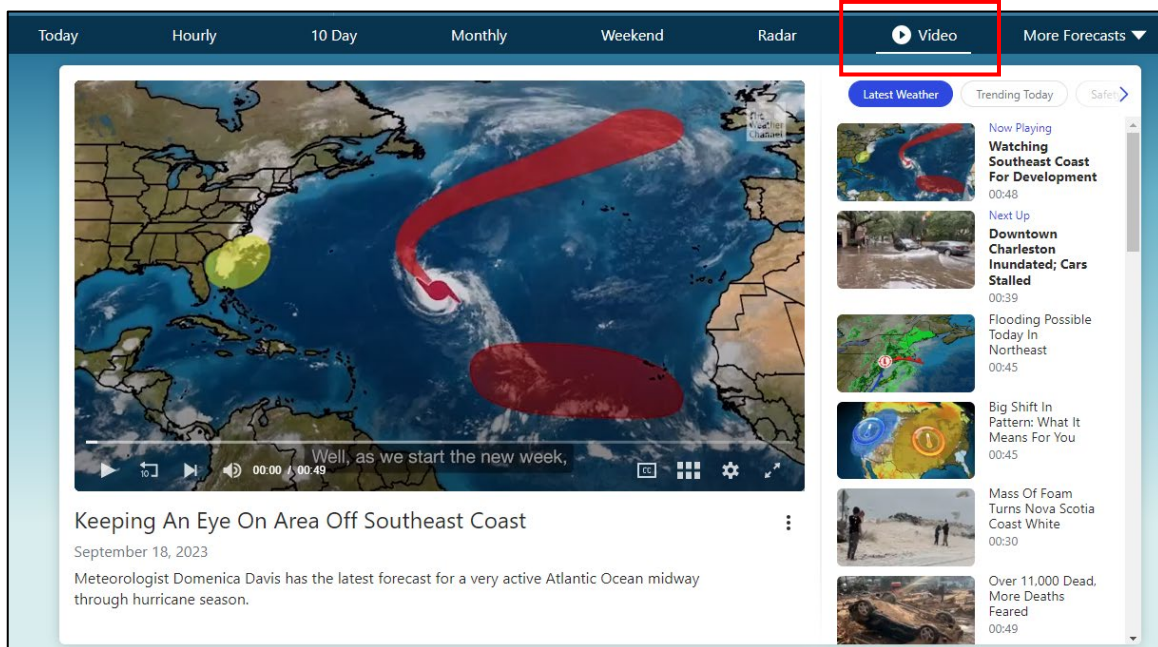
I. DEFENDANT IS A VIDEO TAPE SERVICE PROVIDER

19. Defendant is one of the largest technology companies in the world.

20. One of Defendant’s ventures, is the Weather Channel Website, which prides itself on being “America's #1 Weather Network” with a “daily focus on climate news and best-in-class severe weather coverage.”¹ In more recent years, the Weather Channel has also focused on providing more entertainment-based ventures, such as *Wake Up With Al [Roker]*.

21. Weather.com was visited over 1.2 billion times in May 2023 alone.²

22. While The Weather Channel television network provides live broadcasts, the Website focuses on the provision of pre-recorded, weather-related content. This content can be found under a “Video” tab on the Website:



¹ <https://www.weathergroup.com/brands/the-weather-channel>.

² <https://www.similarweb.com/website/weather.com/#overview>

23. Through its operation of the Website, Defendant is a “video tape service provider,” 18 U.S.C. § 2710(a)(4), because the provision of pre-recorded video content is “a focus of the [D]efendant’s work.” *In re Vizio, Inc., Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1221 (C.D. Cal. 2017).

II. DEFENDANT KNOWINGLY DISCLOSES CONSUMERS’ PERSONALLY IDENTIFIABLE INFORMATION TO THIRD PARTIES, AND WILLFULLY PROCURES THIRD PARTIES TO INTERCEPT THE CONTENTS OF WEBSITE COMMUNICATIONS

A. Testing Reveals That Defendant Illegally Shares Its’ Consumers PII And Video-Viewing Information With Third Parties, And That Third Parties, As Procured By Defendant, Intercept The Contents Of Website Users’ Communications

24. In Summer 2023, Plaintiff’s counsel retained a private research company to review the Website and conduct a dynamic analysis. A “dynamic analysis” records the transmissions that occur from a user’s device or web browser.

25. The researchers tested what information (if any) was disclosed when a user visits the Website and watches a pre-recorded video or takes other actions (*e.g.*, clicking on various menu options). The analysis revealed Defendant disclosed information to third parties sufficient to identify specific Class Members and the specific videos they watched, and that Defendant procured third parties to intercept in real time the content of Class Members’ communications with the Website.

26. The analysis first established that Defendant incorporates multiple “application programming interfaces” (“APIs”) into the Website.

27. APIs “enable[] companies to open up their applications’ data and functionality to external third-party developers, business partners, and internal departments within their companies.”³

28. Crucially, these third party APIs are run and administered by the third parties themselves, rather than being tools through which Defendant records its own data. Likewise, when Defendant sends data to these third parties through their APIs, it is not simply being sent to Defendant’s own servers.

29. As relevant here, Defendant provides mParticle⁴ and AdNexus/Xandr⁵ access to Website data through their respect APIs. The mParticle API provides extensive customer analytics, while AdNexus/Xandr is a major advertising and marketing platform.

30. The dynamic analysis found that when a user views a video on the Website, Defendant transmits to these third parties information sufficient to permit an ordinary person to identify a specific person’s video-viewing behavior, and the content of a user’s communications with the Website is intercepted in real time by these third parties, as procured by Defendant.

31. Specifically, when a user creates a Website account and views a video on the Website, the following information is intercepted by or transmitted to the third parties, mParticle and AdNexus/Xandr:

³ APPLICATION PROGRAMMING INTERFACE (API), <https://www.ibm.com/cloud/learn/api>.

⁴ <https://www.mparticle.com/>

⁵ <https://about.ads.microsoft.com/en-us/solutions/xandr/xandr-premium-programmatic-advertising>

<i>THIRD PARTY</i>	<i>VIDEO INFO</i>	<i>PERSONAL INFO</i>	<i>OTHER INFO</i>
mParticle	Name, URL	geolocation, email, gender, name	
AdNexus	Name	geolocation, email, gender, name	AAID

1. Overview Of mParticle

32. mParticle is “one of the leading customer data platforms, serving hundreds of global brands and helping them turn data to insights, and insights to action.”⁶

33. At a high level, mParticle uses the data it receives and collects from the Website to, among other things, provide “real-time personalization and targeting,” provide “predictive,” “AI-powered insights ... on each customer profile that inform how to preempt churn, improve return on ad spend, and more.”⁷

34. When a Website account user views a video on the Website, Defendant discloses to mParticle, and mParticle—as procured by Defendant—intercepts and collects in real-time, at least the following information: (i) a user’s name and gender, (ii) a user’s e-mail address, (iii) a user’s precise geolocation, (iv) the name of the pre-recorded video watched by the user, and (v) the URL of the pre-recorded video watched by the user, which also contains the name of the video:

⁶ <https://www.mparticle.com/about-us/>

⁷ <https://www.mparticle.com/solutions/real-time-personalization-targeting/>.

We observed mParticle receiving:

Video Information in the form of:

- Video Name, URL, Playlist

Personal Information in the form of:

- Geolocation, Email, Gender, Name

Other Information such as:

- User ID



WITH ACCOUNT

```
POST https://mparticle.weather.com/webevents/v3/JS/us2-fb061d169ced8343850163112c402d41/events
{
  "events": [
    {
      "event_type": "custom_event",
      "data": {
        "event_name": "video-started",
        "timestamp_unixtime_ms": 1692994139011,
        "session_start_unixtime_ms": 1692992931667,
        "custom_attributes": {
          "pageKey": "video",
          "url": "/news/weather/video/extreme-heat-can-cause-roads-to-buckle-blow-out",
          "deviceClass": "desktop",
          "referrer": "https://weather.com/",
          "wlocCity": "Santa Clara",
          "wlocState": "CA",
          "wlocCountry": "US",
          "hourOfDay": 13,
          "dayOfWeek": "FRI",
          "productId": "f787c0bd-3e25-4103-88f0-6423de1fe92f",
          "contentId": "a534d5b5-d874-4edb-81d9-bd0b40c39bde",
          "duration": "00:25",
          "teaserTitle": "Roads Buckling Under Extreme Heat",
          "collection": "news/weather",
          "playlists": [
            "p1-breaking-news",
            "p1-wunderground-top-stories",
            "p1-weather-explained-topic",
            "p1-the-latest",
            "p1-samsung"
          ],
          "title": "Extreme Heat Can Cause Roads To Buckle, Blow Out",
          "seoTitle": "Extreme Heat Can Cause Roads To Buckle, Blow Out | Weather.com",
          "pageCount": 2,
          "location": {
            "latitude": 37.35,
            "longitude": -121.95
          },
          "mp_deviceid": "a3acc055-e56b-40fa-c781-baa5d02738be",
          "device_info": {
            "platform": "web",
            "screen_width": 2560,
            "screen_height": 1080
          },
          "user_attributes": {
            "gender": "M",
            "sfirstName": "Bravericko",
            "emailSubscriptions": {},
            "premium": false,
            "premiumProductTier": null,
            "premiumExpiration": null,
            "premiumStart": null,
            "premiumFirstTransactionDate": null,
            "premiumProductAutoRenew": null,
            "isRegisteredUser": false,
            "devUser": false,
            "Amplitude_device_id": "c22209ab-4ddb-4cfd-8a41-cbe7b5f9e1e0",
            "user_identities": {
              "other": "e239d378-7e3c-4452-9e94-17b0af52691b",
              "customer_id": "62a608aa607141ffb99ef7ee0a06914a",
              "email": "bravericko2876@gmail.com"
            }
          }
        }
      }
    }
  ]
}
```

35. mParticle intercepts this information as soon as a user clicks on and loads a pre-recorded video (*i.e.*, contemporaneously with the communication).

2. Overview Of AdNexus/Xandr

36. AdNexus/Xander is a premium advertising platform.⁸ At a high level, AdNexus/Xander uses the data it receives and collects from the Website to, among other things, “help advertisers engage with audiences using ... digital video,”⁹ analyze the effectiveness of advertising campaigns,¹⁰ and “monetize proprietary data.”¹¹

37. When a Website account user views a video on the Website, Defendant discloses

⁸ <https://about.ads.microsoft.com/en-us/solutions/xandr/xandr-premium-programmatic-advertising>

⁹ <https://about.ads.microsoft.com/en-us/solutions/xandr/advertiser-platform-invest-dsp-premium-content>.

¹⁰ *Id.*

¹¹ <https://about.ads.microsoft.com/en-us/solutions/xandr/curation-platform-self-serve-monetization-solution>

to AdNexus/Xander, and AdNexus/Xander—as procured by Defendant—intercepts and collects in real-time, at least the following information: (i) a user’s name and gender, (ii) a user’s e-mail address, (iii) a user’s precise geolocation, and (iv) the name of the pre-recorded video watched by the user:

We observed **Adnxs** receiving:

Video Information in the form of:

- Video Name

Personal Information in the form of:

- Geolocation, Email, Gender, Name

Other Information such as:

- AAID



WITH ACCOUNT

```
GET https://secure.adnxs.com/getuid?https://match.sharethrough.com/sync/v1?source_id=8e8893f9b606c9c5d33f1be
{
  "data": {
    "custom_event_type": "other",
    "event_name": "module-viewed",
    "custom_attributes": {
      "moduleId": "WxuContentMedia-sidebar-bd88006a-fed4-498d-8241-e7c6050fac3f",
      "pageTitle": "Watch Pavement Blow Out",
      "pageId": "home",
      "dayOfWeek": "FRI",
      "locale": "en-US",
      "deviceClass": "desktop",
      "referrer": "https://weather.com/",
      "wlocCity": "New York City",
      "wlocCountry": "US",
      "wlocState": "NY",
      "regime": "usa-ccpa",
      "hourOfDay": 13
    },
    "location": { "latitude": 37.35, "longitude": -121.95 },
    "mp_deviceid": "784d2fd0-27d5-4986-67fe-c433575da370",
    "user_attributes": {
      "$gender": "M",
      "$firstName": "Bravericko",
      "isRegisteredUser": true,
      "Amplitude.device_id": "dc674501-84c7-480e-983e-041bbdbb7c0b"
    },
    "user_identities": {
      "other": "e239d378-7e3c-4452-9e94-17b8af52691b",
      "customer_id": "62a608aa607141ffb99ef7ee0a06914a",
      "email": "bravericko2876@gmail.com"
    },
    "consent_state": {
      "gdpr": {
        "sensitiveData": { "consented": true, "document": "sensitiveData", "timestamp_unixtime_ms": 1692994073324 }
      },
      "ccpa": {
        "data_sale_opt_out": { "consented": false, "document": "priv_sale_of_data", "timestamp_unixtime_ms": 1692994073324 }
      }
    }
  }
}
```

38. AdNexus/Xander intercepts this information as soon as a user clicks on and loads a pre-recorded video (*i.e.*, contemporaneously with the communication).

B. Defendant Discloses PII To Third Parties, And Third Parties, As Procured By Defendant, Intercept The Content Of Users’ Communications

39. The VPPA prohibits the “knowing[] diclos[ure]” by a “video tape service provider” of the “personally identifiable information concerning any consumer of such provider.” 18 U.S.C. § 2710(b)(1). “[T]he term ‘personally identifiable information’ includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provide.” 18 U.S.C. § 2710(a)(3).

40. Likewise, the MWESCA prohibits the “[w]illful[] intercept[ion] [of] ... any wire,

oral, or electronic communication.” Md. Code Cts. & Jud. Proc. § 10-402(a)(1). “Intercept” is defined as “the aural or other acquisition of the contents of any [] electronic ... communication.” Md. Code Cts. & Jud. Proc. § 10-401(4). And “[c]ontents” is defined as “any information concerning *the identity of the parties to the communication* or the existence, substance, purport, or meaning of that communication.” Md. Code Cts. & Jud. Proc. § 10-401(7) (emphasis added).

41. Thus, to be liable under the VPPA or the MWESCA, the third party must receive or collect information sufficient to identify a particular user. As alleged below, the names, e-mail addresses, and precise geolocation disclosed to and collected by mParticle and AdNexus/Xandr fit the bill.

1. *Defendant Discloses Users’ Names And E-Mail Addresses To Third Parties, And Third Parties Intercept Users’ Names And E-Mail Addresses*

42. Without a doubt, someone’s full name is sufficient to identify a particular person. However, the same is true of an e-mail address.

43. An email address is a unique string of characters which designate an electronic mailbox. As industry leaders,¹² trade groups,¹³ and courts agree,¹⁴ an ordinary person can use an email address to uniquely identify another individual. Indeed, there exists multiple services that

¹² Allison Schiff, *Can Email Be The Next Big Online Identifier?*, AD EXCHANGER (Aug. 25, 2020), <https://www.adexchanger.com/data-exchanges/can-email-be-the-next-big-online-identifier/> (quoting Tom Kershaw, CTO of Magnite, who said “[a]n email address is universally considered to be PII, so as such it can never be a valid identifier for online advertising”).

¹³ NETWORK ADVERTISING INITIATIVE, NAI CODE OF CONDUCT 19 (2019), https://thenai.org/wp-content/uploads/2021/07/nai_code2020.pdf (identifying email as PII).

¹⁴ *See, e.g., United States v. Hastie*, 854 F.3d 1298, 1303 (11th Cir. 2017) (“Email addresses fall within the ordinary meaning of information that identifies an individual. They can prove or establish the identity of an individual.”).

enable anyone with internet access and a credit card to look up who owns a particular email address.¹⁵

44. mParticle also admits an “email address is more likely to be unique to a single user than [some other identifiers].”¹⁶

45. As the dynamic analysis establishes, when a user with an account watches a pre-recorded video on the Website, Defendant discloses users’ names and e-mail addresses to mParticle and AdNexus/Xandr, and mParticle and AdNexus/Xandr collect users’ names and e-mail addresses contemporaneously with the communication (*i.e.*, with clicking on and watching a pre-recorded video).

46. Geolocation is “the identification of the real-world geographic location of an object.”¹⁷ Geolocation identifies an object by “generating a set of geographic coordinates such a latitude and longitude through GPS and using the coordinates to determine a meaningful location.”¹⁸

2. *Defendant Discloses Users’ Precise Geolocation To Third Parties, And Third Parties Intercept Users’ Precise Geolocation*

47. Geolocation is considered precise when it provides street level accuracy. Defendant discloses—and third parties intercept—such precise geolocation here. Specifically, Defendant discloses to mParticle and AdNexus/Xandr—and mParticle and AdNexus/Xandr intercept in transit—users’ geolocation with more than three decimal places of accuracy, meaning mParticle and AdNexus/Xandr could identify users within forty feet of their actual

¹⁵ See, e.g., www.beenverified.com.

¹⁶ <https://docs.mparticle.com/guides/idsync/identify-users/>

¹⁷ WHAT IS GEOLOCATION?, <https://www.indicative.com/resource/geolocation/>.

¹⁸ WHAT IS GEOLOCATION?, <https://www.indicative.com/resource/geolocation/>.

location.

48. Precise geolocation can be used by anyone to uniquely identify a person. A study in 2013, for example, analyzed mobility data for 1.5 million people, finding that researchers needed only four randomly chosen spatio-temporal points (points that represent the time and location of a specific event, such as watching a video) to uniquely identify 95% of the people (approximately 1.425 million out of 1.5 million) in the dataset.¹⁹

49. This data may also be used to track consumers to sensitive locations, including places of religious worship, places that may be used to infer an LGBTQ+ identification, domestic abuse shelters, medical facilities, and welfare and homeless shelters.

50. By plotting the latitude and longitude coordinates including geolocation data using publicly available map programs, it is possible to identify which consumers' mobile devices visited reproductive health clinics. Similar methods may be used to trace consumers' visits to other sensitive locations.

51. As Paul Ohm, a law professor and privacy researcher at Georgetown University Law Center, explains it: “[r]eally precise, longitudinal geolocation information is absolutely impossible to anonymize.”²⁰ In fact, out of all identifiers, “D.N.A. is probably the only thing that’s harder to anonymize than precise geolocation information.”²¹

¹⁹ Yves-Alexandre de Montjaye, et al., *Unique in the Crowd: The privacy bounds of human mobility*, SCIENTIFIC REPORTS 2 (Feb. 4, 2013), <https://www.nature.com/articles/srep01376>.

²⁰ Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy* N.Y. TIMES (Dec. 19, 2019), <https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html>.

²¹ *Id.*

52. By disclosing users' geolocation data to third parties, and by procuring third parties to collect geolocation, Defendant discloses or otherwise procures third parties to collect information that an ordinary person could use to identify Defendant's users.²²

53. Companies collect and disclose geolocation so they can maximize their advertising revenue. As a *New York Times* article explained: "For brands, following someone's precise movement is key to understanding the 'customer's journey'—every step of the process from seeing an ad to buying a product."

54. Marketers consider geolocation "the Holy Grail of advertising" because it creates "the complete picture that connects all of our interests and online activity with our real-world actions."²³

55. Defendant's conduct is self-serving, as mParticle and AdNexus/Xandr use the geolocation they collect and receive to enhance Defendant's marketing efforts, advertising, and Website analytics.

3. *Defendant Discloses Information Identifying Which Specific Videos Were Watched By Which Specific Users, And Third Parties Intercept Information Identifying Which Specific Videos Were Watched By Which Specific Users*

56. As alleged above, Defendant discloses the full names of the pre-recorded videos watched by Website users to mParticle and AdNexus/Xandr, and mParticle and AdNexus/Xandr intercept in transit the full names of the pre-recorded videos watched by Website users.

²² See *Yershov v. Gannett Satellite Info. Network, Inc.*, 820 F.3d 482, 486 (1st Cir. 2016).

²³ *Id.*

57. In addition, Defendant discloses the URL of the pre-recorded videos watched by Website users to mParticle, and mParticle intercepts in transit URL s of the pre-recorded videos watched by Website users. The URL discloses the exact name of the pre-recorded video, as indicated by the snippet of Website traffic recorded in the analysis:

```

"url": "/news/weather/video/extreme-heat-can-cause-roads-to-buckle-blow-out",
"deviceClass": "desktop",
"referrer": "https://weather.com/",
"wlocCity": "Santa Clara",
"wlocState": "CA",
"wlocCountry": "US",
"hourOfDay": 13,
"dayOfWeek": "FRI",
"productId": "f787ccbd-3e25-4103-88f0-6423de1fe92f",
"contentId": "a534d5b5-d874-4edb-81d9-bd0b40c39bde",
"duration": "00:25",
"teaserTitle": "Roads Buckling Under Extreme Heat",
"collection": "news/weather",
"playlists": ["pl-breaking-news", "pl-wunderground-top-stories", "pl-weather-explained-Topic", "pl-the-latest", "pl-samsung"],
"title": "Extreme Heat Can Cause Roads To Buckle, Blow Out"

```

* potential video IDs

58. The transmission and collection of this video information occurs when a user actually watches the specific pre-recorded video, and not simply because a user visits a page with a video and does not watch the video, or visits a page with many videos and the information does not indicate which video is watched.

59. *First*, both mParticle and AdNexus/Xandr receive the *full name* of the video, not just the URL. Thus, it is clear from that transmission the title of the video watched by the user, not just that a user visited a page with a video.

60. *Second*, the transmissions to mParticle and AdNexus/Xandr indicate that a video was indeed watched. For instance, the mParticle transmission specifically includes the value “event name” : “video started,” as well as the time when that video was watched:

```

"data": {
  "event_name": "video-started",
  "timestamp_unixtime_ms": 1692994139011,
  "session_start_unixtime_ms": 1692992931667,
  "custom_attributes": {
    "pageKey": "video",
    "url": "/news/weather/video/extreme-heat-can-cause-roads-to-buckle-blow-out"
  }
}

```

61. The time stamp value is a Unix Timestamp, which “is a way to track time as a running total of seconds. This count starts at the Unix Epoch on January 1st, 1970 at UTC. Therefore, the unix time stamp is merely the number of seconds between a particular date and the Unix Epoch.”²⁴ The time stamp here—1692994139011—is August 25, 2023 at 4:08:59 p.m. Eastern Time.²⁵

62. Similarly, for AdNexus/Xandr, the network traffic shows the value, “‘event_name’ : ‘module-viewed’,” being transmitted, where “module” refers to the video watched. This is clear from the value, “‘moduleTitle,’” which is the name of the video:

```

"data": {
  "custom_event_type": "other",
  "event_name": "module-viewed",
  "custom_attributes": {
    "moduleId": "WxuContentMedia-sidebar-bd88006a-fed4-498d-8241-e7c6050fac3f", * potential video ID
    "moduleTitle": "Watch Pavement Blow Out",
  }
}

```

63. Thus, mParticle and AdNexus/Xandr not only receive and collect what specific video a user watches, but also that the user in fact watched a specific video.

C. Defendant Discloses Personally Identifiable Information To Third Parties For The Purpose Of Marketing, Advertising, And Website Analytics

64. Defendant discloses PII to mParticle and AdNexus/Xandr, and otherwise procures mParticle and AdNexus/Xandr to intercept the contents of users’ Website communications, so mParticle and AdNexus/Xandr can help Defendant with marketing, advertising, and analytics.

65. As alleged above, mParticle and AdNexus/Xandr are designed to analyze Website data, conduct targeted marketing and advertising, and ultimately boost Defendant’s revenue from its video-based marketing and advertising on the Website.

²⁴ THE CURRENT EPOCH UNIX TIMESTAMP, <https://www.unixtimestamp.com/>.

²⁵ *Id.*

1. *Defendant Discloses Personally Identifiable Information To mParticle, And Defendant Procures mParticle To Intercept The Contents Of Website Communications, For The Purpose Of Marketing, Advertising, And Website Analytics*

66. As alleged above, mParticle describes itself as a “as one of the leading customer data platforms, serving hundreds of global brands and helping them turn data to insights, and insights to action.”²⁶

67. One of mParticle’s key features is “IDSync,” “[t]he primary purpose of [which] is to ensure that you are attributing data to the correct user, *which requires you to successfully identify the current user of your app or website.*”²⁷

68. mParticle notes that “[a]s soon as the user opens your app [or website], an identity request is automatically made to mParticle to look for a matching user profile.”²⁸ mParticle also admits that it receives “the username or email address provided when the user signs up,” and uses that information to track users.²⁹

69. Crucially, the default configuration for mParticle is only to collect a user’s “customer ID.”³⁰ Therefore, Defendant had to knowingly and willfully allow mParticle to receive and collect e-mail addresses and geolocation data because otherwise, mParticle would only be receiving and collecting customer IDs.

70. Once a user has been identified, their actions are tracked across a website like Defendant’s, and that “event data” is used to measure website performance and statistics. Website

²⁶ <https://www.mparticle.com/about-us/>.

²⁷ <https://docs.mparticle.com/guides/idsync/identify-users/> (emphasis added).

²⁸ *Id.* (emphasis added).

²⁹ *Id.*

³⁰ <https://docs.mparticle.com/guides/idsync/default-strategy/>

developers like Defendant can configure mParticle to receive and collect “custom event” data, which covers a wide assortment of activity on a website.³¹

71. Ironically, the example for “custom event data” mParticle lists in its developer documentation is “Videos Watched”:

Capture a Custom Event

You can quickly log a simple event as follows:

```

1  mParticle.logEvent(
2    'Video Watched',
3    mParticle.EventType.Navigation,
4    {'category': 'Destination Intro', 'title': 'Paris'}
5  );
```

72. mParticle also allows website developers like Defendant to “track the location of your users.”³² Again, this is an optional feature, meaning Defendant has to knowingly and willfully allow and procure mParticle to receive and collect geolocation data.

73. With all of this event and location data, mParticle, ironically again, shows website developers like Defendant how they can violate the VPPA (and the MWESCA). In mParticle’s developer documentation, it includes the following tutorial:

The mPTravel app lets users watch video content about travel destinations. This tutorial creates an audience to allow mPTravel to *target users who view content about a particular destination with deals for that destination.*³³

74. *First*, mParticle would record the “event data” for whoever watched a specific video.³⁴

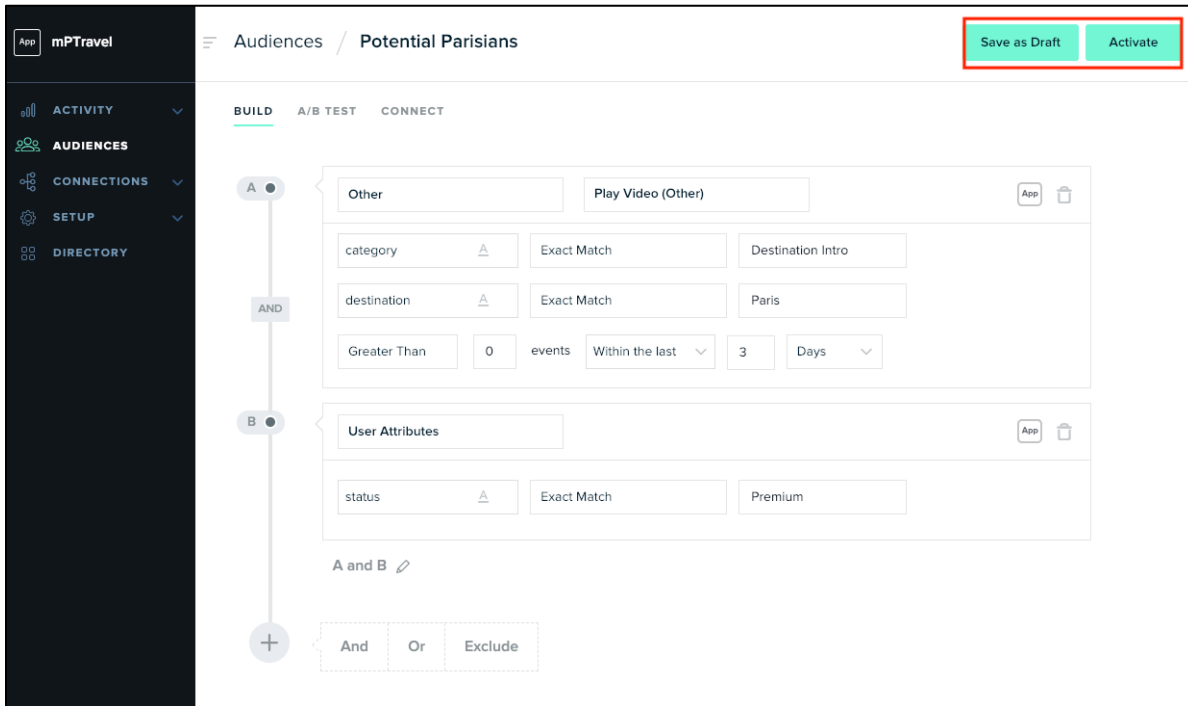
³¹ <https://docs.mparticle.com/developers/sdk/web/event-tracking/>

³² <https://docs.mparticle.com/developers/sdk/web/location/>

³³ <https://docs.mparticle.com/guides/getting-started/create-an-audience/> (emphasis added).

³⁴ <https://docs.mparticle.com/guides/getting-started/create-an-audience/>

75. *Second*, mParticle can include in its “Audience” whoever clicks on and watches that specific video, as well as other attributes like subscription status, geolocation, or any attribute the website developer wants to send or have mParticle collect.³⁵



76. *Third*, once a website developer “activates” this “audience,” mParticle will begin receiving, collecting, and measuring data that matches the criteria listed above. So, as applied to Defendant’s Website, Defendant might create an “audience” of users who watched a specific video from a specific location, and mParticle would receive and collect that data (as well as users’ names and e-mail addresses).

77. *Fourth*, after receiving and collecting sufficient data, mParticle can forward the “audience” to another third party to conduct marketing. So, in the above example, mParticle could

³⁵ *Id.*

forward the contact information for all “audience” members to Mailchimp, who would send targeted e-mail advertising to users based on the specific video they watched.³⁶

78. All of this is to benefit website developers like Defendant, who send data to mParticle and otherwise procure mParticle to intercept communications to drive website traffic, conduct targeted marketed campaigns using detailed user data, and increase revenue (*e.g.*, through incentivizing users to purchase products on a website through targeted advertising).

79. The receipt and collection of this user data also allows mParticle to identify users and build sophisticated user profiles, encompassing everything from a user’s name and location to age range and gender³⁷:

The screenshot displays the mParticle Profile API Demo interface. The left sidebar contains navigation options: ACTIVITY (Overview, User Activity, System Alerts, Event Forwarding, GDPR Requests), DATA MASTER, AUDIENCES, CONNECTIONS, SETUP, and DIRECTORY. The main content area shows the profile for 'Example-Customer-mxr15' under 'User Activity'. It features three sections: 'Devices', 'User Attributes', and 'Audience Membership'.

Device ID	Is Limit Ad Tracking On?	Input	Last Seen	Push Token
481c8a31-7d5d-4d96-93a0-2de7427167fc	No	Android	1 hour ago	--
f52bfb9e-bf36-4309-b372-9ab7a5488027	No	MobileWeb	1 hour ago	--

\$City	\$Country	\$FirstName	\$LastName
New York	USA	Marky	Mark
\$State	churn_risk_score	last_purchase_category	ltv
NY	4	Home Decor	342.1
ml_product_recs	tp_age	tp_gender	view_preference
123849,294933,937592,500422	18-34	male	Dark Mode

The 'Audience Membership' section shows an audience named 'Workwear Launch Campaign 17807'.

80. Defendant uses and procures each and every one of the above-mentioned features of mParticle, among others, on the Website. Thus, Defendant discloses data to mParticle, and

³⁶ <https://docs.mparticle.com/guides/getting-started/connect-an-audience-output/>.

³⁷ <https://www.mparticle.com/platform/detail/profile-api/>

procures mParticle to intercept user data, to perform extensive Website analytics, conduct targeted marketing campaigns, and improve Website performance—all of which, in turn, generates greater revenue for Defendant.

2. *Defendant Discloses Personally Identifiable Information To AdNexus/Xandr, And Defendant Procures mParticle To Intercept The Contents Of Website Communications, For The Purpose Of Marketing, Advertising, And Website Analytics*

81. As alleged above, AdNexus/Xander is a premium advertising platform now owned by Microsoft, and is part of the suite of interest advertising services offered by Microsoft.³⁸

82. In particular:

The Xandr platform is a real-time bidding system and ad server. The main processing system is called the “impression bus.” The impression bus receives ad requests, applies data to the request, receives bids, makes decisions, serves creatives, logs auctions, etc.

Ad calls come in via our inventory supply partners: exchanges, SSPs, ad networks, and a few valued publishers.

...

Once we get the call, we overlay segment data from our server-side cookie store. Data is added to the cookie store either through Xandr segment pixels or by clients sending us a file of data. We also contact third-party data providers and overlay any available data.

We contact all of the bidders on our platform. The ad call includes whatever user data belongs to each bidder, and information about the inventory. Bidders have a certain number of milliseconds in which to respond with a bid and the creative they want to serve.

...

The impression bus decides which bid wins based on the amount of the bid, and any preferences the publisher has about what they want served on their page.³⁹

³⁸ <https://about.ads.microsoft.com/en-us/solutions/xandr/xandr-premium-programmatic-advertising>

³⁹ https://docs.xandr.com/bundle/invest_invest-standard/page/topics/about-invest.html

83. To break this down, “real-time bidding” or “RTB” is the process through which advertisers and marketers “buy[] and sell[] ads in real time” to website and mobile users. After receiving relevant user data, “multiple advertisers [] bid on a single impression of a publisher’s inventory, then the winning ad (with the highest bid) is shown to the user.”⁴⁰ As an example:

[t]ake ... the moment in a mobile game where the player watches an ad between game levels. At that moment, the mobile [supply-side platform or SSP] runs an auction for all of the advertisers interested in showing an ad to that player. The advertisers make their bid and, in a split-second, the highest bidder is chosen. Their advertisement is then served to the player.⁴¹

84. As AdNexus/Xandr notes, there are several key players in the RTB process, which include but are not limited to:

- (a) Publishers (sellers) provide inventory, or the space where ads are displayed. This may be a website or a mobile app.
- (b) Advertisers or marketers (buyers) purchase inventory for the display of advertisements. For example, Microsoft, Amazon, and Target are all advertisers.
- (c) Users are the target customers for advertisements.
- (d) Supply Side Platforms (SSPs) enable publishers to access demand from many different networks, exchanges, and platforms through a single interface. For example, Xandr, Liverail, OpenX, and Pubmatic can act as SSPs.⁴²

85. Each of these entities work together to serve targeted advertisements to users in a process called “ad serving.” To elaborate, “[a]d serving is the process of determining which advertisement goes in which ad slot on a publisher's webpage or mobile app and then delivering the advertisement.”⁴³

⁴⁰ <https://www.adjust.com/glossary/real-time-bidding/>

⁴¹ *Id.*

⁴² <https://docs.xandr.com/bundle/industry-reference/page/introduction-to-ad-serving.html>

⁴³ *Id.*

86. AdNexus/Xander is a real-time bidding platform (specifically, a SSP) that facilitates this economy. It provides “targeting, bidding algorithms, multi-currency support, and all the other features of a premium ad server.”⁴⁴

87. A website like Defendant’s uses or procures AdNexus/Xander to maximize revenue by having advertisers bid on which ads will be shown to website users, and then show those users targeted marketing and advertisements based on the user’s personal data.

88. To facilitate the RTB process, however, AdNexus/Xander needs to receive and collect an enormous amount of data about website users. For instance, one of AdNexus/Xander’s features is “Geo Radius Segments.” “A geo radius segment is a list of latitude, longitude, and radius data. [A website developer] can use geo radius segments for geographical targeting of multiple user locations.”⁴⁵ Thus, if a website developer sends geolocation data to AdNexus/Xander, and/or AdNexus/Xander intercepts said data, AdNexus/Xander can create segments of users based on their geolocation. That geolocation data—or users fitting within a certain geolocation-based segment—would then be shown to advertisers, who would use AdNexus/Xander’s RTB platform to bid on showing advertisements relevant to a user’s location to each user.

89. Crucially, “Geo Radius Segments” is an optional feature of AdNexus/Xander, meaning Defendant had to knowingly and willfully enable this feature to disclose and procure AdNexus/Xander to intercept geolocation data.

90. Another feature of AdNexus/Xander—although one that is apparently in a “closed beta”—is “video content targeting.” Through this feature, AdNexus/Xander can target users

⁴⁴ https://docs.xandr.com/bundle/invest_invest-standard/page/topics/about-invest.html

⁴⁵ https://docs.xandr.com/bundle/monetize_monetize-standard/page/topics/geo-radius-segments.html

“based on available detail about the specific video content, including the type of programming, the subject matter, the scheduled airtime, and more.”⁴⁶

91. Given Defendant discloses video-viewing information to AdNexus/Xander, it appears as though the Website is part of the optional, “closed beta.” Thus, Defendant has AdNexus/Xander target users with specific advertisements based on which videos they watch. And, again, this is an optional beta Defendant appears to be part of.

92. Defendant uses and procures each and every one of the above-mentioned features of AdNexus/Xandr on the Website. Thus, Defendant discloses data to AdNexus/Xandr, and procures AdNexus/Xandr to intercept user data, to facilitate real-time bidding, serve targeted advertisements on users based on their PII, and generate greater revenue for Defendant through this process.

D. Defendant Knowingly Discloses Its Consumers’ PII To mParticle And AdNexus/Xandr, And Willfully Procures mParticle And AdNexus/Xandr To Intercept The Content Of Website Users’ Communications

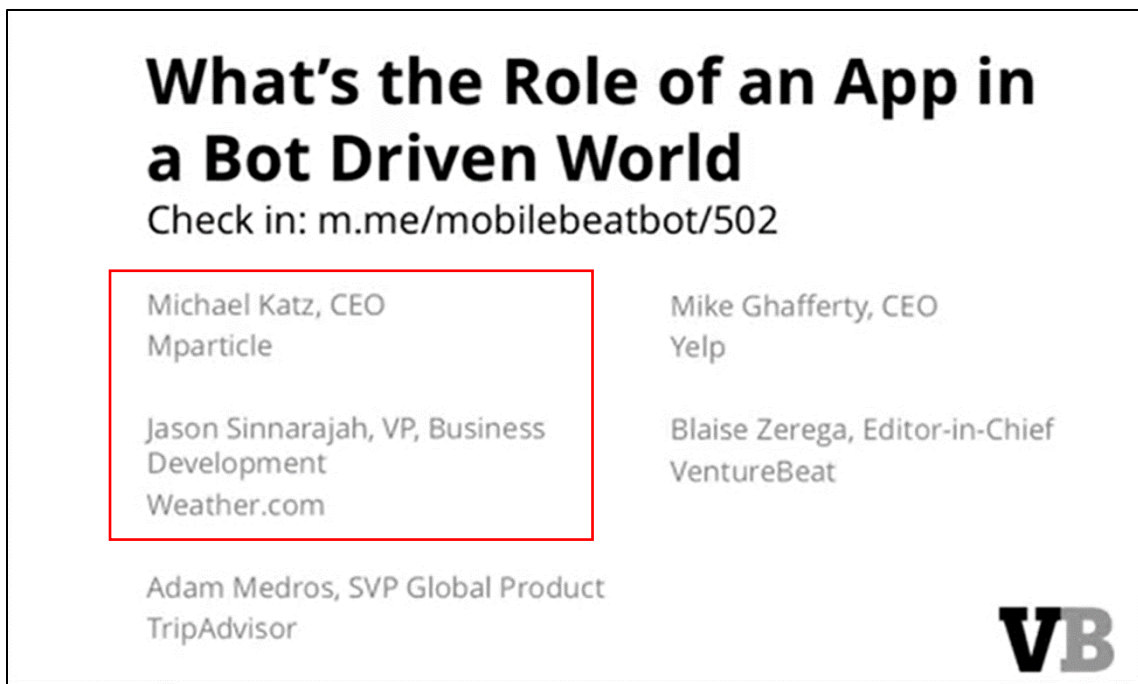
93. Based on the above, it is abundantly clear that Defendant *knowingly* discloses its users’ personally identifiable information to mParticle And AdNexus/Xandr. Likewise, it is abundantly clear that Defendant *willfully* procures mParticle And AdNexus/Xandr to intercept the content of Website users’ communications.

94. Naturally, mParticle And AdNexus/Xandr have access to Website user data through Defendant’s efforts; mParticle And AdNexus/Xandr do not simply appear on Defendant’s Website. Accordingly, Defendant must knowingly and willfully allow mParticle And AdNexus/Xandr to collect the aforementioned user data.

⁴⁶ https://docs.xandr.com/bundle/monetize_monetize-standard/page/topics/video-content-targeting.html

95. Further, Defendant has enabled many optional features of mParticle and AdNexus/Xandr that allow these third parties to collect additional user data, such as e-mail addresses, geolocation, and video-viewing information.

96. Dispelling any doubt, Defendant has, for instance, had its executives appear at conferences and talks with mParticle’s CEO⁴⁷:



97. Likewise, mParticle lists “The Weather Channel” as a user of mParticle’s “Button” feature, which “provides a way for mobile brands to partner with one another, creating the only simple, scalable, and accurate approach to mobile affiliate acquisition and commerce.”⁴⁸

CLASS ALLEGATIONS

98. Pursuant to Fed. R. Civ. P. 23(a) and 23(b)(3), Plaintiff seeks to represent a class of all United States residents who visited Weather.com during the statute of limitations period,

⁴⁷ <https://www.youtube.com/watch?v=e0PbpWMYRFY>

⁴⁸ <https://www.mparticle.com/blog/button-partnership/>

created an account on the Website, and watched a pre-recorded video (the “Nationwide Class”).

99. Plaintiff seeks to represent a class of all Maryland residents who visited Weather.com in Maryland during the statute of limitations period, created an account on the Website, watched a pre-recorded video in Maryland, and had the contents of their electronic communications intercepted or recorded by mParticle and/or AdNexus/Xandr (the “Maryland Subclass”).

100. The Nationwide Class and Maryland Subclass shall be collectively referred to as the “Class.”

101. Plaintiff reserves the right to modify the class definition as appropriate based on further investigation and discovery obtained in the case.

102. Members of the Class are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Class number in the thousands. The precise number of Class Members and their identities are unknown to Plaintiff at this time but may be determined through discovery. Class Members may be notified of the pendency of this action by mail and/or publication through the distribution records of Defendants.

103. Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Common legal and factual questions include, but are not limited to, whether Defendant violated the VPPA, whether Defendant violated the MWESCA, whether Defendant has been unjustly enriched, and whether class members are entitled to actual and/or statutory damages for the aforementioned violations.

104. The claims of the named Plaintiff are typical of the claims of the Class because the named Plaintiff, like all other class members, visited the Weather.com, created an account, and watched a pre-recorded video on the Website.

105. Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the Class Members she seeks to represent, she has retained competent counsel experienced in prosecuting class actions, and she intends to prosecute this action vigorously. The interests of Class Members will be fairly and adequately protected by Plaintiff and her counsel.

106. The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of Class Members. Each individual Class Member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

107. Plaintiff brings all claims in this action individually and on behalf of members of the Class against Defendant.

CAUSES OF ACTION

COUNT I
Violation Of The VPPA,
18 U.S.C. § 2710

108. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

109. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

110. Defendant is a “video tape service provider” as defined by the VPPA because it “engage[s] in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials,” 18 U.S.C. § 2710(a)(4), inasmuch as it provides video (*i.e.*, “similar audio visual materials” under the VPPA’s definition) to consumers via its Website. Specifically, Defendant provides pre-recorded, weather-related videos to consumers on the Website.

111. Plaintiff and Class Members are “consumers” as defined by the VPPA because they created Website accounts, through which they provided Defendant (and, without consent, the third parties mentioned in this Complaint) their names and e-mail addresses, which were used to track Plaintiff and Class Members when they viewed video content. 18 U.S.C. § 2710(a)(1). Under the VPPA, therefore, Plaintiff and members of the Classes are “subscribers” of “goods or services [the Website, which provides pre-recorded video content] from a video tape service provider.” 18 U.S.C. § 2710(a)(1).

112. That is, through their creation of an account on Defendant’s Website, the purpose of which is to provide pre-recorded video content to users, Plaintiff and Class Members provided additional information (their names and e-mail addresses) that was used to track them without their consent, and therefore are “subscribers” because they registered, committed and expressed association with the Website.

113. Plaintiff and Class Members viewed pre-recorded videos on the Website. During each of these occasions, Defendant disclosed Plaintiff’s and Class Members PII. Specifically:

- (a) Plaintiff’s and Class Members’ (i) full names, (ii) e-mail addresses, (iii) precise geolocation, (iv) the name of the pre-recorded video

watched by Plaintiff and Class Members, and (iv) the URL of the pre-recorded video watched by Plaintiff and Class Members, which also contains the name of the video, were disclosed to mParticle.

- (b) Plaintiff's and Class Members' (i) full names, (ii) e-mail addresses, (ii) precise geolocation, and (iii) the name of the pre-recorded video watched by Plaintiff and Class Members, and were disclosed to AdNexus/Xandr.

114. The Website's transmissions of Plaintiff's and Class Members' PII to mParticle and AdNexus/Xandr constitute "knowing[] disclosures" of Plaintiff's and Class Members' "personally identifiable information" to a person as proscribed by the VPPA. 18 U.S.C. § 2710(a)(1).

115. Under the VPPA, the term "personally identifiable information" "includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3). The information disclosed by Defendant constitutes "personally identifiable information" because it allows an ordinary person to identify Plaintiff and Class Members, as well as which specific videos were watched by Plaintiff and each Class Member.

116. Plaintiff and Class Members did not provide Defendant with any form of consent—either written or otherwise—to disclose their PII to third parties in violation of the VPPA.

117. Nor were Defendant's disclosures made in the "ordinary course of business" as the term is defined by the VPPA. In particular, the Apps' disclosures to mParticle and AdNexus/Xandr were not necessary for "debt collection activities, order fulfillment, request processing, [or] transfer of ownership." 18 U.S.C. § 2710(a)(2).

118. On behalf of herself and the Class, Plaintiff seeks: (i) declaratory relief; (ii) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with VPPA's requirements for protecting a consumer's PII; (iii) statutory damages of \$2,500 for each violation of the VPPA pursuant to 18 U.S.C.

§ 2710(c); and (iv) reasonable attorneys' fees, costs, and other litigation expenses.

COUNT II

**Violation Of The Maryland Wiretapping And Electronic Surveillance Act,
Md. Code Cts. & Jud. Proc. §§ 10-401, *et seq.***

119. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

120. Plaintiff brings this claim individually and on behalf of the members of the proposed Maryland Subclass against Defendant.

121. The MWESCA makes it unlawful for any person to “[w]illfully intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication.” Md. Code Cts. & Jud. Proc. § 10-402(a)(1).

122. In the context of the MWESCA, “willfully” is defined as “an intentional violation or a reckless disregard of a known legal duty.” *Benford v. Am. Broadcasting Co.*, 649 F. Supp. 9, 10 (D. Md. 1986).

123. “Electronic communication” is defined as “[a]ny transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system.” Md. Code Cts. & Jud. Proc. § 10-401(5)(i).

124. “Intercept” is defined as “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” Md. Code Cts. & Jud. Proc. § 10-401(4).

125. “Contents” is defined as “any information concerning *the identity of the parties to the communication* or the existence, substance, purport, or meaning of that communication.” Md. Code Cts. & Jud. Proc. § 10-401(7) (emphasis added).

126. As alleged above, mParticle and AdNexus/Xandr, as procured by Defendant, intercepted Plaintiff's and Maryland Subclass Members' electronic communications because mParticle and AdNexus/Xandr, through their APIs, "reroute[d] communications to the interceptor[s]," mParticle and AdNexus/Xandr respectively. *Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 130 (3d Cir. 2022); see also *Katz-Lacabe v. Oracle America, Inc.*, --- F. Supp. 3d ---, 2023 WL 2838118, at *9 (N.D. Cal. Apr. 6, 2023) (finding plaintiffs sufficiently alleged a third-party data analytics company was a third-party wiretapper under California law).

127. Further, as alleged above, mParticle and AdNexus/Xandr intercepted the "contents" of Plaintiff's and the Maryland Subclass's electronic communications with Defendant because mParticle and AdNexus/Xandr intercepted information concerning "the identity of the parties to the communication" (*i.e.*, the names, e-mail addresses, and geolocation of Plaintiff and other Maryland Subclass Members, which is sufficient to identify them).

128. mParticle and AdNexus/Xandr also intercepted the "contents" of Plaintiff's and the Maryland Subclass's electronic communications with Defendant because mParticle and AdNexus/Xandr intercepted the "substance, purport, or meaning" of Plaintiff's and Maryland Subclass Members' communications (*i.e.*, the specific videos viewed by Plaintiff and Maryland Subclass Members).

129. Plaintiff's and Maryland Subclass Members' electronic communications were intercepted in Maryland, which is "the point at which the signals [*i.e.*, Plaintiff's and the Maryland Subclass's electronic communications] were routed to [mParticle's and AdNexus/Xandr's] servers." *Popa*, 52 F.4th at 132.

130. At all relevant times, Defendant procured mParticle and AdNexus/Xandr to intercept Plaintiff's and Maryland Subclass Members' electronic communications with

Weather.com.

131. Defendant sought to profit and in fact did profit off procuring the interception of Plaintiff's and the Maryland Subclass Members' electronic communications while intentionally or recklessly disregarding its known legal duty.

132. Specifically, Defendant was enriched when it utilized Plaintiff's and Class members' personal information for its own financial advantage to optimize its own platform, including by allowing its partners to target Plaintiff and Maryland Subclass Members for lucrative advertisements. Defendant also profited when it utilized Plaintiff's and Class members' personal information stored without meaningful consent for its own financial advantage to build better services, to maintain and improve its services, to develop new services, and to measure performance, all of which enable Defendant to create operational efficiencies and be competitive in a wide array of industries.

133. In exchange for Plaintiff's and Maryland Subclass Members loss of privacy and the financial benefits Defendant enjoyed as a result thereof, including, but not limited to, advertising profits, while Plaintiff and Maryland Subclass Members received nothing.

134. Plaintiff and Maryland Subclass Members did not provide their prior consent to Defendant's actions in procuring mParticle and AdNexus/Xandr to wiretap visitors to Weather.com. Nor did Plaintiff or Maryland Subclass Members meaningfully consent to mParticle's and AdNexus/Xandr's intentional access, interception, reading, learning, recording, and collecting of Plaintiff's and Maryland Subclass Members' electronic communications.

135. The violation of MWESCA constitutes an invasion of privacy sufficient to confer Article III standing. *See generally Bohnak v. Marsh & McLennan Cos.*, --- F.4th ---, 2023 WL 5437558 (2d Cir. Aug. 24, 2023); *see also In re Facebook Internet Tracking Litigation*, 956 F.3d

589, 598-99 (9th Cir. 2020).

136. Plaintiff and Maryland Subclass Members seek all relief available under Md. Code Cts. & Jud. Proc. §§ 10-410(a)(1)-(3), including statutory damages of \$100 dollars per day for each day of violation or \$1,000, whichever is higher, punitive damages, and reasonable attorneys' fees and costs.

COUNT III
Unjust Enrichment

137. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

138. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

139. Plaintiff brings this claim pursuant to the laws of the State of Maryland.

140. Plaintiff and Class Members unwittingly conferred a benefit upon Defendant. Defendant took and retained valuable personal location information belonging to Plaintiffs and Class Members when it disclosed to third parties, or otherwise procured third parties to intercept, Plaintiff's and Class Members' personally identifiable information and the contents of Plaintiff's and Class Members' Website communications without their consent.

141. Defendant was enriched when it utilized Plaintiff and Class Members' names, e-mail addresses, and precise geolocation information without consent for Defendant's own financial advantage to optimize its advertising and analytics efforts, including by allowing its paying advertisers to target Plaintiff and Class Members for lucrative advertisements based on videos they had viewed, and to analyze Website data to drive traffic and increase revenue.

142. Defendant was enriched when it utilized Plaintiffs and Class Members' names, e-mail addresses, and precise geolocation information without consent for its own financial

advantage to build better services, to maintain and improve Defendant's services, to facilitate the real-time bidding process, and to measure performance, all of which enable Defendant to, and which Defendant does use, to create operational efficiencies and be compete with its competitors.

143. In exchange for Plaintiff's and Class Members' loss of privacy and the financial benefits Defendant enjoyed as a result thereof, including, but not limited to, advertising profits, Plaintiff and Class Members received nothing.

144. It would be inequitable for Defendant to retain the benefits it has unjustly received. Therefore, as a result of Defendant's actions, Plaintiff and Class Members seek an order that Defendant disgorge the profits and other benefits it has unjustly obtained.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests, individually and on behalf of all others similarly situated, seek judgment against Defendant, as follows:

- (a) For an order certifying the Nationwide Class and the Maryland Subclass under Rule 23 of the Federal Rules of Civil Procedure, naming Plaintiff as the representative of the Nationwide Class and the Maryland Subclass, and naming Plaintiff's attorneys as Class Counsel to represent the Nationwide Class and the Maryland Subclass;
- (b) For an order declaring the Defendant's conduct violates the statutes referenced herein;
- (c) For an order finding in favor of Plaintiff, the Nationwide Class, and the Maryland Subclass on all counts asserted herein;
- (d) For compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury;
- (e) For prejudgment interest in all amounts awarded;
- (f) For an order of restitution and all other forms of equitable monetary relief;
- (g) For an order awarding Plaintiff, the Nationwide Class, and the Maryland Subclass their reasonable attorneys' fees and expenses and cost of suit.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of any and all issues in this action so triable as of right.

Dated: September 19, 2023

Respectfully submitted,

BURSOR & FISHER, P.A.

By: /s/ Joseph I. Marchese
Joseph I. Marchese

Joseph I. Marchese
Max S. Roberts
Julian C. Diamond
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-Mail: jmarchese@bursor.com
mroberts@bursor.com
jdiamond@bursor.com

BURSOR & FISHER, P.A.

Christopher R. Reilly*
701 Brickell Ave., Suite 1420
Miami, FL 33131
Telephone: (305) 330-5512
Facsimile: (305) 676-9006
E-Mail: creilly@bursor.com

**Pro Hac Vice forthcoming*

Attorneys for Plaintiff