

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

FRANCIS LUCCHESI-SOTO, KEVIN
MCGUIRE, MATTHEW WICKHAM, and
AMITAI HELLER, individually and on behalf
of all others similarly situated,

Plaintiffs,

v.

THE CRITERION COLLECTION, LLC,

Defendant.

Case No. 1:24-cv-07345

**FIRST AMENDED CLASS
ACTION COMPLAINT**

JURY TRIAL DEMANDED

Hon. Valerie E. Caproni

Dated: April 14, 2025

BURSOR & FISHER, P.A.

Yitzchak Kopel

Max S. Roberts

Victoria X. Zhou

1330 Avenue of the Americas, 32nd Floor

New York, NY 10019

Telephone: (646) 837-7150

Facsimile: (212) 989-9163

E-Mail: ykopel@bursor.com

mroberts@bursor.com

vzhou@bursor.com

LEVI & KORSINSKY, LLP

Mark S. Reich

Gary S. Ishimoto*

33 Whitehall Street, Floor 17

New York, NY 10004

Telephone: (212) 363-7500

Facsimile: (212) 363-7171

Email: mreich@zlk.com

Email: gishimoto@zlk.com

**Pro Hac Vice Forthcoming*

Attorneys for Plaintiffs

TABLE OF CONTENTS

	PAGE
NATURE OF THE ACTION	1
FACTUAL BACKGROUND	2
I. HISTORY AND OVERVIEW OF THE STATUTES	2
A. The VPPA	2
B. The Federal, Pennsylvania, and Florida Wiretapping Acts	3
II. DEFENDANT IS A VIDEO TAPE SERVICE PROVIDER	5
III. DEFENDANT DISCLOSES SUBSCRIBERS’ PERSONALLY IDENTIFIABLE INFORMATION TO THIRD PARTIES	6
A. Testing Reveals That Defendant Illegally Discloses Subscribers’ PII To Twilio And Meta	6
B. Defendant Discloses Subscribers’ Full Names to Twilio	9
C. Defendant Discloses Subscribers’ E-Mail Addresses To Twilio	11
D. Defendant Discloses Subscribers’ User IDs and Android Advertising IDs to Twilio	12
E. Defendant Discloses Website Subscribers’ Meta IDs to Meta	15
F. Defendant Discloses Subscribers’ Video-Viewing Information to Twilio and Meta	20
IV. DEFENDANT DISCLOSES SUBSCRIBERS’ PII TO THIRD PARTIES FOR THE PURPOSES OF MARKETING, ADVERTISING, AND ANALYTICS	24
A. Defendant Discloses Subscribers’ PII To Twilio For Marketing, Advertising, And Analytics	24
B. Defendant Discloses Subscribers’ PII To Meta For Marketing, Advertising, And Analytics	27
VI. EXPERIENCES OF PLAINTIFFS	30
A. Plaintiff Francis Lucchese-Soto	30

B.	Plaintiff Kevin McGuire	31
C.	Plaintiff Matthew Wickham.....	32
D.	Plaintiff Amitai Heller	33
THE PARTIES.....		34
JURISDICTION AND VENUE		35
CLASS ALLEGATIONS		35
CAUSES OF ACTION		38
COUNT I		38
COUNT II		40
COUNT III.....		43
COUNT IV		45
PRAYER FOR RELIEF		47
JURY DEMAND		47

Plaintiffs Francis Lucchese-Soto, Kevin McGuire, Matthew Wickham, and Amitai Heller (“Plaintiffs”), individually and on behalf of all other persons similarly situated, by and through their attorneys, make the following allegations pursuant to the investigation of their counsel and based upon information and belief, except as to allegations specifically pertaining to themselves and their counsel, which are based on personal knowledge.

NATURE OF THE ACTION

1. This is a class action suit brought against Defendant The Criterion Collection, LLC (“Criterion” or “Defendant”) for violating the Video Privacy Protection Act (“VPPA”), 18 U.S.C. § 2710, the Electronic Communications Privacy Act (the “Federal Wiretap Act” or “ECPA”), 18 U.S.C. § 2510, the Pennsylvania Wiretapping and Electronic Surveillance Control Act (“WESCA”), 18 Pa. Cons. Stat. §§ 5701, *et seq.*, and the Florida Security of Communications Act (“FSCA”), Fla. Stat. §§ 934.01, *et seq.*

2. Criterion is an American home-video distribution company that focuses on licensing, restoring, distributing, and streaming classic and contemporary films. In addition to selling physical DVDs and Blu-Ray discs, it also operates the Criterion Channel video streaming service for a monthly cost of \$10.99 (or \$99.99 per year). This subscription allows members to stream certain films on demand and provides access to Criterion24/7, which provides members with a continuous stream of Criterion’s films.

3. Users can stream the Criterion Channel through its website: <https://www.criterionchannel.com/> (the “Website”). The Criterion Channel also has a mobile application available on Android and iOS devices (the “App”).¹ The App and the Website are collectively referred to as the “Criterion Channel Service.”

¹ The App shall refer to both the Android and iOS version, unless otherwise specified.

4. The Criterion Channel is available in the United States and Canada.

5. Unbeknownst to Plaintiffs and members of the Class, Defendant knowingly and intentionally discloses Criterion Channel Service users' personally identifiable information—including a record of every video viewed by the user—to unrelated third parties. By doing so, Defendant is violating the VPPA, the Federal Wiretapping Act, WESCA, and the FSCA.

6. Plaintiffs bring this action for damages and other legal and equitable remedies resulting from Defendant's violations of the VPPA, the Federal Wiretapping Act, WESCA, and the FSCA.

FACTUAL BACKGROUND

I. HISTORY AND OVERVIEW OF THE STATUTES

A. The VPPA

7. The impetus for the VPPA begins with President Ronald Reagan's nomination of Judge Robert Bork to the United States Supreme Court. During the confirmation process, a movie rental store disclosed the nominee's rental history to the Washington City Paper which then published that record. Congress responded by passing the VPPA, with an eye toward the digital future. As Senator Patrick Leahy, who introduced the Act, explained:

It is nobody's business what Oliver North or Robert Bork or Griffin Bell or Pat Leahy watch on television or read or think about when they are home. In an area of interactive television cables, the growth of computer checking 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 profile of a person and tell what they buy in a store, what kind of food they like, what sort of television programs they watch, who are some of the people they telephone. I think that is wrong.

S. Rep. 100-599, at 5-6 (1988) (cleaned up).

8. In 2012, Congress amended the VPPA, and in so doing, reiterated the VPPA's

applicability to “so-called ‘on-demand’ cable services and Internet streaming services [that] allow consumers to watch movies or TV shows on televisions, laptop computers, and cell phones.” S. Rep. 112-258, at 2 (2012).

9. The VPPA prohibits “[a] video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider.” 18 U.S.C. § 2710(b)(1). The VPPA defines personally identifiable information (“PII”) as “information which identifies a person as having requested or obtained specific video materials or services from a video service provider.” 18 U.S.C. § 2710(a)(3). A video tape service provider is “any person, engaged 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).

10. As the Second Circuit has held, “[t]he VPPA is no dinosaur statute ... Our modern means of consuming content may be different, but the VPPA’s privacy protections remain as robust today as they were in 1988.” *Salazar v. Nat. Basketball Association*, 118 F.4th 533, 553 (2d Cir. 2024).

B. The Federal, Pennsylvania, and Florida Wiretapping Acts

11. The original Federal Wiretap Act was enacted in 1934 “as a response to Fourth Amendment concerns surrounding the unbridled practice of wiretapping to monitor telephonic communications.” Hayden Driscoll, *Wiretapping the Internet: Analyzing the Application of the Federal Wiretap Act’s Party Exception Online*, 29 WASH. & LEE J. C.R. & SOC. JUST. 187, 192 (2022).

12. The Wiretap Act primarily concerned the government’s use of wiretaps, but Congress grew concerned that technological advancements like “large-scale mail operations,

computer-to-computer data transmissions, cellular and cordless telephones, paging devices, and video teleconferencing” were rendering the Wiretap Act out of date. S. Rep. No. 99-541, at 2 (1986). Thus, in 1986, Congress amended the Wiretap Act through the ECPA to provide a private right of action for private sector intrusions as though they were government intrusions. Driscoll, 29 WASH. & LEE J. C.R. & SOC. JUST. at 192.

13. Title I of the ECPA amended the Wiretap Act such that a violation occurs when a person or entity: (i) provides an electronic communication service to the public; and (ii) intentionally divulges the contents of any communication; (iii) while the communication is being transmitted on that service; (iv) to any person or entity other than the intended recipient of such communication.

14. While the ECPA allows a single party to consent to the interception of an electronic communication, single party consent is only acceptable where the communication is not “intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.” 18 U.S.C. § 2511(2)(d).

15. In the wake of the ECPA, many states also passed wiretapping laws of their own, including Pennsylvania and Florida.

16. Pennsylvania’s WESCA has its roots in the common law right to privacy, which protects citizens’ “protectable interest in their private information and ... the sanctity of their communications.” *Petris v. Sportsman’s Warehouse, Inc.*, 2024 WL 2817530 (W.D. Pa. June 3, 2024)

17. WESCA operates in conjunction with and as a supplement to the Federal Wiretap Act, which allows states to “grant greater, but not lesser, protection than that available under federal law.” *Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 124 (3d Cir. 2022). WESCA does

so by prohibiting: (i) the intentional interception of wire, electronic, or oral communication; (ii) the intentional disclosure of the contents of any wire, electronic or oral communication, or evidence derived therefrom to another person; and (iii) the intentional use of the contents of any wire, electronic or oral communication, or evidence derived therefrom. 18 Pa. C.S. § 5703(a).

18. As the Third Circuit has held, “the WESCA is to be strictly construed to protect individual privacy rights.” *Popa*, 52 F.4th at 129.

19. Florida has a similar privacy protection statute. To establish a claim under the FSCA, the persons bringing suit must be Florida residents, or the improper interception must have occurred in Florida. West’s F.S.A. §§ 934.02(5), 934.10(1).

20. The FSCA makes it illegal for a person to “intentionally intercept[], endeavor[] to intercept, or procure[] any other person to intercept or endeavor to intercept any wire, oral or electronic communication.” Fla Stat. § 934.03(1)(a). Further, the FSCA prohibits the “use,” “disclosure” or any endeavors to use or disclose the contents of such intercepted communications. Fla. Stat. § 934.03(1)(b)-(e).

II. DEFENDANT IS A VIDEO TAPE SERVICE PROVIDER

21. Criterion, via the Criterion Channel Service, provides:

an independent streaming service that features an eclectic mix of classic and contemporary films from Hollywood and around the world, many not available anywhere else. In addition to hosting the Criterion Collection and Janus Films’ celebrated library of more than 1,500 films, it also features titles from a wide array of studio and independent licensors and original programming exclusive to the service. Along with the constantly refreshed thematic programming, subscribers to the Criterion Channel Service can also enjoy more than 500 shorts and 5,000 supplementary features, including trailers, introductions, behind-the-scenes documentaries, interviews, video essays, commentary tracks, and rare archival footage.²

² FAQ, CRITERION, <https://www.criterion.com/faq/channel>.

22. In short, the Criterion Channel contains pre-recorded videos that are available for users who purchase a subscription to watch.

23. To receive access to the Criterion Channel Service, a user must specifically register for it. To access the Criterion Channel Service through a paid subscription or a free trial, a user must provide his or her “name, e-mail address, billing address, or credit card number.”³ Users pay either \$10.99 per month or \$99.99 per year, and a paid subscription is required to access Criterion Channel’s pre-recorded videos.

24. Those that pay for a subscription to the Criterion Channel Service shall hereinafter be referred to as “Subscribers.”

25. The Criterion Channel Service is available throughout the United States and Canada.

26. The Criterion Channel App has over 100,000 downloads on the Google Play Store alone.⁴

III. DEFENDANT DISCLOSES SUBSCRIBERS’ PERSONALLY IDENTIFIABLE INFORMATION TO THIRD PARTIES

A. Testing Reveals That Defendant Illegally Discloses Subscribers’ PII To Twilio And Meta

27. In August 2024, prior to the commencement of this action, Bursor & Fisher retained a private research company to conduct a dynamic analysis of the App and Website. A “dynamic analysis” records the transmissions that occur from a user’s device.

28. The private researchers tested what information (if any) Defendant discloses when

³ PRIVACY, CRITERION, <https://www.criterionchannel.com/privacy>; *see also* CHECKOUT, CRITERION, <https://www.criterionchannel.com/checkout/subscribe/purchase>.

⁴ *See* CRITERION CHANNEL, GOOGLE PLAY STORE, https://play.google.com/store/apps/details?id=com.criterionchannel&hl=en_US.

a user watches a pre-recorded video on the Criterion Channel Service.

29. The analysis first established that Defendant incorporates multiple “application programming interfaces” (“APIs”) and “software development kits” (“SDKs”) into the Website and App.

30. APIs “enable[] companies to open up their applications’ data and functionality to external third-party developers, business partners, and internal departments within their companies.”⁵ An API can “work[] as a standalone solution or included within an SDK. ... [A]n SDK often contains at least one API.”⁶ “SDK stands for software development kit and “is a set of software-building tools for a specific program, while “API” stands for application programming interface.”⁷ As used in this Complaint, “SDK” and “API” are referring to the same software.

31. Defendant integrates into its Website and App the Segment API/SDK (“Segment”), which is owned and operated by Twilio Inc. (“Twilio”).

32. Twilio is “a customer engagement platform” used by hundreds of thousands of businesses that allows businesses to “[e]mbrace every customer personally on a single platform.”⁸

33. Twilio powers this platform through Segment, which offers “world-class customer data infrastructure, so [developers] can design hyper-personalized, omnichannel campaigns across all channels.”⁹

⁵ APPLICATION PROGRAMMING INTERFACE (API), <https://www.ibm.com/cloud/learn/api>.

⁶ SDK VS. API: WHAT’S THE DIFFERENCE?, IBM (July 13, 2011), <https://www.ibm.com/blog/sdk-vs-api/>.

⁷ *Id.*

⁸ TWILIO, <https://tinyurl.com/yc4udmea>.

⁹ TWILIO + SEGMENT ARE BETTER TOGETHER WITH TWILIO ENGAGE, TWILIO SEGMENT, <https://segment.com/twilio/>.

34. Once integrated into a developer’s mobile application, the Segment API provides Twilio’s platform with “customer identification and segmentation.”¹⁰ It does this by “collecting and connecting data from other tools and aggregating the data to monitor performance, inform decision-making processes, and create uniquely customized user experiences.”¹¹

35. The dynamic analysis found that when Criterion Channel Service users with a paid account watch a pre-recorded video on the Website, Defendant discloses a user’s PII to Twilio, as follows:

THIRD PARTY	VIDEO INFO	PERSONAL INFO	OTHER INFO
Segment	Video Title, Video ID, Video Url	Email (unhashed), Full Name	User ID

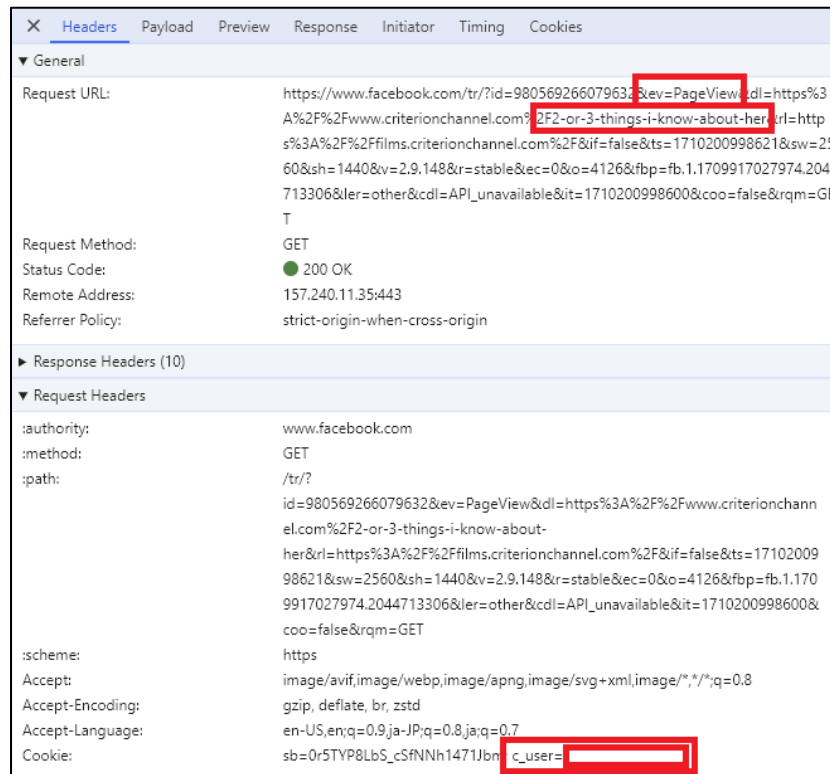
36. Similarly, the dynamic analysis also found that when Criterion Channel Service users with a paid account watch a pre-recorded video on the App, Defendant discloses a user’s PII to Twilio, as follows:

THIRD PARTY	VIDEO INFO	PERSONAL INFO	OTHER INFO
Segment	Video Title, Video ID, Video Interactions	Email (unhashed), Full Name	User ID, AAID

¹⁰ Ingrid Lunden, *Twilio Confirms It Is Buying Segment For \$3.2b In An All-Stock Deal*, TECHCRUNCH, Oct. 12, 2020, <https://techcrunch.com/2020/10/12/twilio-confirms-it-is-buying-segment-for-3-2b-in-an-all-stock-deal/>.

¹¹ SEGMENT.IO DEFINED, INDICATIVE, <https://www.indicative.com/resource/segment-io/>.

37. Testing by Levi & Korsinsky prior to the commencement of this action also found that previously, when Website users requested or obtained pre-video content on the Website while being simultaneously signed into an existing Meta Platforms, Inc. account, Defendant discloses to Meta Platforms, Inc. (“Meta” and collectively with Twilio, the “Third Parties”) through the Meta Pixel its Subscribers’ (i) c_user cookie, which contains a user’s unencrypted and unique Facebook ID (“FBID” or “Meta ID”), and (ii) the full title of the video watched:



B. Defendant Discloses Subscribers’ Full Names to Twilio

38. As the below excerpts of the dynamic analysis show, Defendant discloses to Twilio a user’s full name when a user watches a pre-recorded video on the Criterion Channel Service:

```

timezone: America/New York
name: Penelope Strickland
email: biimamamama@gmail.com
vimeo_id: 64513575
path: /heisei-era-godzilla/season:1/videos/godzilla-vs-biollante
referrer: https://www.criterionchannel.com/heisei-era-godzilla
search:
title: Godzilla vs. Biollante - Heisei-Era Godzilla - The Criterion Channel

```

Defendant's Disclosure of Website Users' Full Names to Twilio

```

"timezone": "America\\New_York",
"traits": {
  "anonymousId": "B07384D0-1310-42CB-A32D-DB342F88BCDE",
  "email": "peppymay@yahoo.com",
  "name": "Penelope Strickland",
  "vimeo_id": "64533512"
},
"userAgent": "ios site\\59054 ios-app\\8.800.1"
},
"event": "Video Playback Paused",
"integrations": {
}

```

Defendant's Disclosure of App Users' Full Names to Twilio (iOS)

```

anonymousId : 0a80a0ac-efca-4c00-983e-3b22eb244e63 ,
"email": "lari.shirokaka@gmail.com",
"name": "Lari Shirokaka",
vimeo_id : 61091066
},
"userAgent": "Dalvik/2.1.0 (Linux; U; Android 12; AOSP on sargo Build/SP2A.220505.008)"
},
"event": "Video Playback Buffer Started",

```

Defendant's Disclosure of App Users' Full Names to Twilio (Android)

39. A user's full name is obviously PII, as it is the exact information of Judge Bork's that was disclosed that led to the enactment of the VPPA in the first place.

//

//

//

//

//

//

C. Defendant Discloses Subscribers' E-Mail Addresses To Twilio

40. An e-mail address is a unique string of characters which designates an electronic mailbox. As industry leaders,¹² trade groups,¹³ and courts¹⁴ agree, an ordinary person can use an e-mail address to uniquely identify another individual. Indeed, there exist multiple services that enable their clients to look up who owns a particular e-mail address.¹⁵

41. As the below excerpts of the dynamic analysis show, Defendant discloses to Twilio a user's e-mail address when a user watches a pre-recorded video on the Criterion Channel Service:

//

//

//

//

//

//

//

//

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 (2020), https://thenai.org/wp-content/uploads/2021/07/nai_code2020.pdf (identifying email as PII).

¹⁴ *See 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.”).

¹⁵ *See, e.g.*, EXPERIAN IDENTITY APPEND, <https://docs.experianaperture.io/identity-append/experian-identity-append/overview/introduction/#reverse-email-append> (“Reverse email append ... allows you to input an email address and receive the name and address of the individual associated with that email.”).

```

user_email: blimalamamama@gmail.com
user_id: 64513575
video_id: 3269060
view: video
session_id: 895aa9bb2fe1b023ae5985bc19353652
collection_title: Heisei-Era Godzilla
video_title: Godzilla vs. Biollante
name: video
name: The Criterion Channel

```

**Defendant's Disclosure of Website
Users' E-Mail Addresses to Twilio**

```

"timestamp": "1.723482093E9",
"type": "video",
"user_email": "peppymay@yahoo.com",
"user_id": "64533512",
"video_id": "3269060",
"video_title": "Godzilla vs. Biollante"
},

```

**Defendant's Disclosure of App
Users' E-Mail Addresses to Twilio (iOS)**

```

"timestamp": "1.723482093E9",
"type": "video",
"user_email": "lari.shirokaka@gmail.com",
"user_id": "61091060",
"video_id": "3308698.0",
"video_title": "Licorice Pizza"
},
"timestamp": "2024-08-12T17:01:33.091Z",
"type": "track"

```

**Defendant's Disclosure of App
Users' E-Mail Addresses to Twilio (Android)**

D. Defendant Discloses Subscribers' User IDs and Android Advertising IDs to Twilio

42. As the following excerpts show, the dynamic analysis also found that Defendant discloses to Twilio the Vimeo ID and/or user ID of Website and App users when a user watches a pre-recorded video on the Criterion Channel Service. Defendant also discloses Android App users' Android Advertising IDs ("AAID") to Twilio:


```

user_id: 64513575
video_id: 3269060
view: video
session_id: 895aa9bb2fe1b023ae5985bc19353652
collection_title: Heisei-Era Godzilla
video_title: Godzilla vs. Biollante
name: video
name: The Criterion Channel
version: None
externalIds: {'collection': 'users', 'encoding': 'none', 'type': 'vimeo_id', 'id': '64513575'}
locale: en-US
timezone: America/New_York
name: Penelope Strickland
email: blimalamamama@gmail.com
vimeo_id: 64513575
path: /heisei-era-godzilla/season:1/videos/godzilla-vs-biollante

```

Defendant's Disclosure of Website Users' Vimeo IDs and User IDs to Twilio

```

"timezone": "America\\New_York",
"traits": {
  "anonymousId": "B07384D0-1310-42CB-A32D-DB342F88BCDE",
  "email": "peppymay@yahoo.com",
  "name": "Penelope Strickland",
  "vimeo_id": "64533512"
},
"userAgent": "ios site\\59054 ios-app\\8.000.1"
},
"event": "Video Playback Paused",
"integrations": {
  ...
}

```

Defendant's Disclosure of App Users' Vimeo IDs and User IDs to Twilio (iOS)

```

"anonymousId": "6a8ba0ac-efca-4c00-983e-3b22e0244e03",
"email": "lari.shirokaka@gmail.com",
"name": "Lari Shirokaka",
"vimeo_id": "61091066"
},
"userAgent": "Dalvik/2.1.0 (Linux; U; Android 12; AOSP on sargo Build/SP2A.220505.008)"
},
"event": "Video Playback Buffer Started",

```

```

"session_id": "3ab79ae5-c910-4714-ab9b-eff7992cf69f",
"site_id": "59054.0",
"timestamp": "1.723482093E9",
"type": "video",
"user_email": "lari.shirokaka@gmail.com",
"user_id": "61091066",
"video_id": "3308698.0",
"video_title": "Licorice Pizza"
},
"timestamp": "2024-08-12T17:01:33.091Z",
"type": "track"
},
...

```

```

"device": {
  "adTrackingEnabled": "true",
  "advertisingId": "aa49149c-8cf1-425c-aa10-903412cd08b8",
  "id": "1335c195d1337d8708fc79cb98c718b9f7bd00df9c2f83e783fe3d82f2504ba7",
  "manufacturer": "Google",
  "model": "AOSP on sargo",
  "name": "sargo",
  "type": "android"
},

```

Defendant's Disclosure of App Users' Vimeo IDs, User Ids, and AAIDs to Twilio (Android)

43. Defendant’s disclosures of these IDs to Twilio, particularly AAIDs, further enables Twilio to ascertain the identity of the Criterion Channel Service user.

44. An AAID is a unique string of numbers which attaches to a device. As the name implies, an AAID is sent to advertisers and other third parties so they can track user activity across multiple mobile applications.¹⁶ So, for example, if a third party collects AAIDs from two separate mobile applications, it can track, cross-correlate, and aggregate a user’s activity on both apps.

45. Although technically resettable, an AAID is a persistent identifier because virtually no one knows about AAIDs and, correspondingly, virtually no one resets that identifier. The fact that the use and disclosure of AAIDs is so ubiquitous evinces an understanding on the part of Defendant and others in the field that they are almost never manually reset by users (or else an AAID would be of no use to advertisers). *See* Byron Tau, MEANS OF CONTROL: HOW THE HIDDEN ALLIANCE OF TECH AND GOVERNMENT IS CREATING A NEW AMERICAN SURVEILLANCE STATE at 175 (2024) (“Like me, most people had no idea about the ‘Limit Ad Tracking’ menu on their iPhones or the AAID that Google had given even Android devices. Many still don’t.”); *see also* *Louth v. NFL Enterprises LLC*, 2022 WL 4130866, at *3 (D.R.I. Sept. 12, 2022) (“While AAID are resettable by users, the plaintiff plausibly alleges that AAID is a persistent identifier because virtually no one knows about AAIDs and, correspondingly, virtually no one resets their AAID.”) (cleaned up).

46. Using publicly available resources, an AAID can track a user’s movements, habits, and activity on mobile applications.¹⁷ Put together, the AAID serves as “the passport for

¹⁶ *See* ADVERTISING ID, <https://support.google.com/googleplay/android-developer/answer/6048248>.

¹⁷ Thomas Tamblyn, *You Can Effectively Track Anyone, Anywhere Just By The Adverts They Receive*, HUFFPOST, Oct. 19, 2017, https://www.huffingtonpost.co.uk/entry/using-just-1000-worth-of-mobile-adverts-you-can-effectively-track-anyone_uk_59e87ccbe4b0d0e4fe6d6be5.

aggregating all of the data about a user in one place.”¹⁸

47. Because an AAID creates a record of user activity, this data can create inferences about an individual, like a person’s political or religious affiliations, sexuality, or general reading and viewing preferences. These inferences, combined with publicly available tools, make AAIDs an identifier that sufficiently permits an ordinary person to identify a specific individual.

E. Defendant Discloses Website Subscribers’ Meta IDs to Meta

48. A Pixel cannot be placed on a website by a third-party. It must be placed directly by or on behalf of the site owner.

49. Once the Pixel is set and activated, it can begin collecting and sharing user activity data as instructed by the website owner.

50. When a Facebook user logs onto Facebook, a “c_user” cookie – which contains a user’s non-encrypted Facebook User ID number (“UID”) – is automatically created and stored on the user’s device for up to a year.¹⁹

51. This means that for Subscribers to the Streaming Service who are also Facebook users, their PII is certain to be shared. Their PII is automatically bundled with their web watching history and disclosed to Facebook when visiting a page with an active Pixel, including the home page.

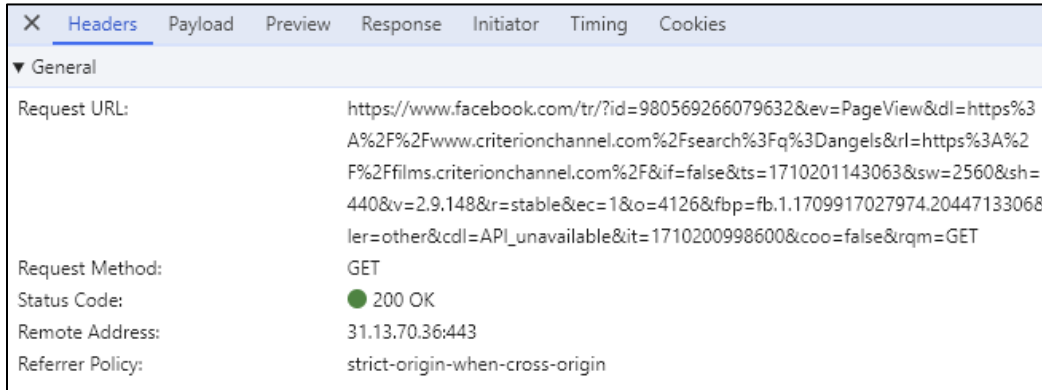
52. While the process to determine what information is being collected by the Pixel from a user is admittedly complicated, the recipient of the Pixel’s transmissions receives the information in a clear and easy to understand manner.

¹⁸ Willie Boag, *Trend Report: Apps Oversharing Your Advertising ID*, IDAC, <https://digitalwatchdog.org/trend-report-apps-oversharing-your-advertising-id/>

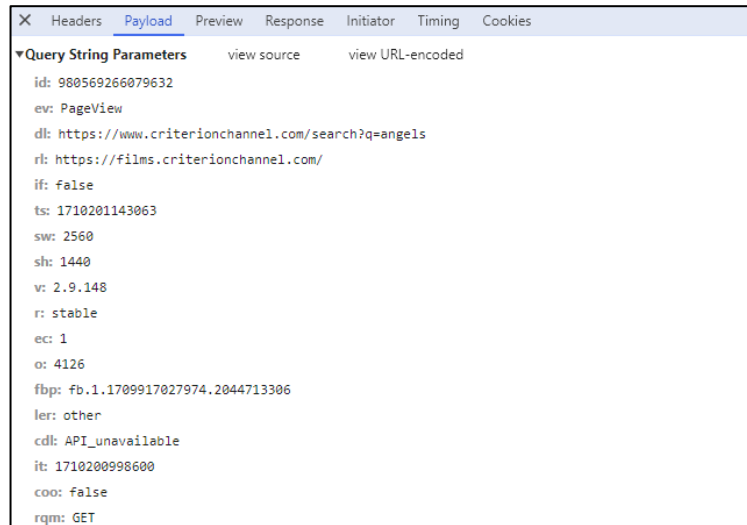
¹⁹ PRIVACY CENTER: COOKIES & OTHER STORAGE TECHNOLOGIES, FACEBOOK, <https://www.facebook.com/policy/cookies/>.

53. The seemingly complex data, such as the long URLs included in the Pixel's transmission, is "parsed" or translated into an easier to read format, such that the information is legible.

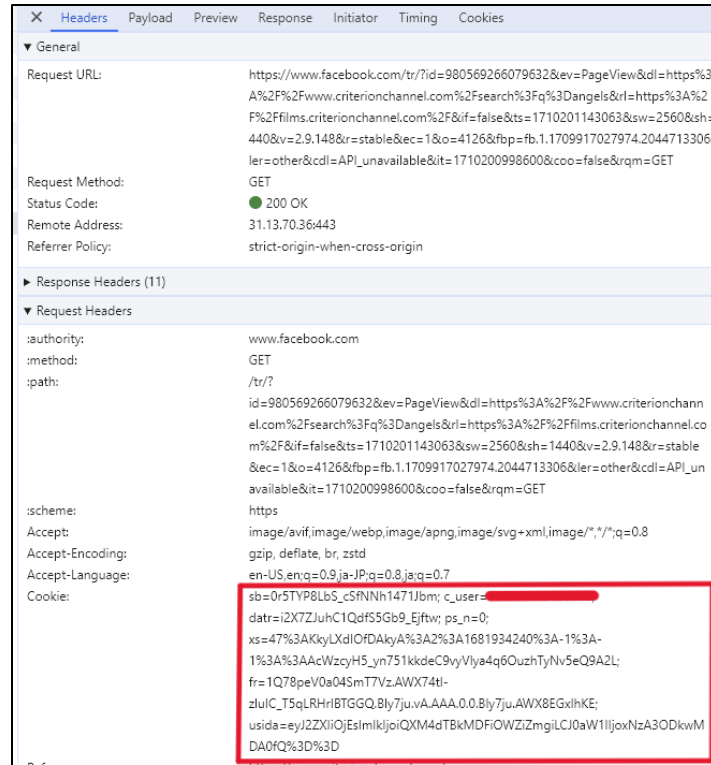
54. For example, an embedded URL in a Pixel HTTP Request may look like an indecipherable code, as depicted below:



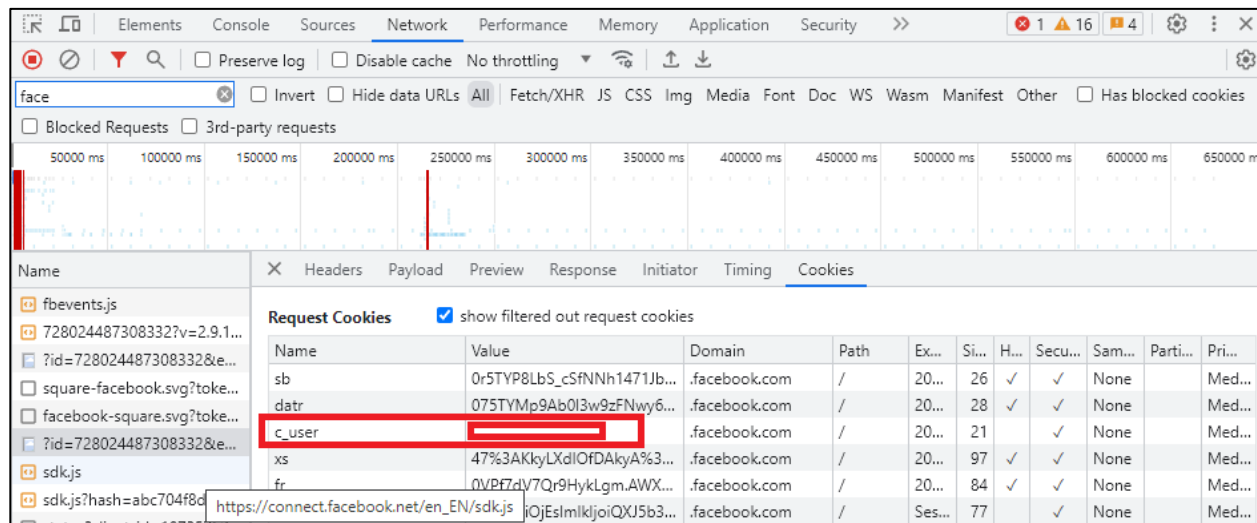
55. However, these URLs are designed to be "parsed" into easy-to-digest pieces of information, as depicted below:



56. Similarly, the cookies attached to the Pixel's transmissions appear as a dense, albeit much less so, wall of text, as depicted below:



57. However, like the URL data, the cookie data is easily parsed into more digestible format, as depicted below:



58. PII can be used by anyone who receives the Pixel transmission to easily identify a Facebook user.

59. A UID is personally identifiable information. It contains a series of numbers used

to identify a specific profile, as depicted below:



c_user=100091959850832;

60. The information contained within the c_user cookie is considered PII. It contains “the kind of information that would readily permit an ordinary person to identify a specific individual’s video-watching behavior.”²⁰ Because the FBID number can simply and easily be appended to “www.facebook.com/” to navigate to the relevant user’s profile, it requires no special skill or expertise to identify the user associated with the FBID, and courts have regularly upheld its status as PII.²¹

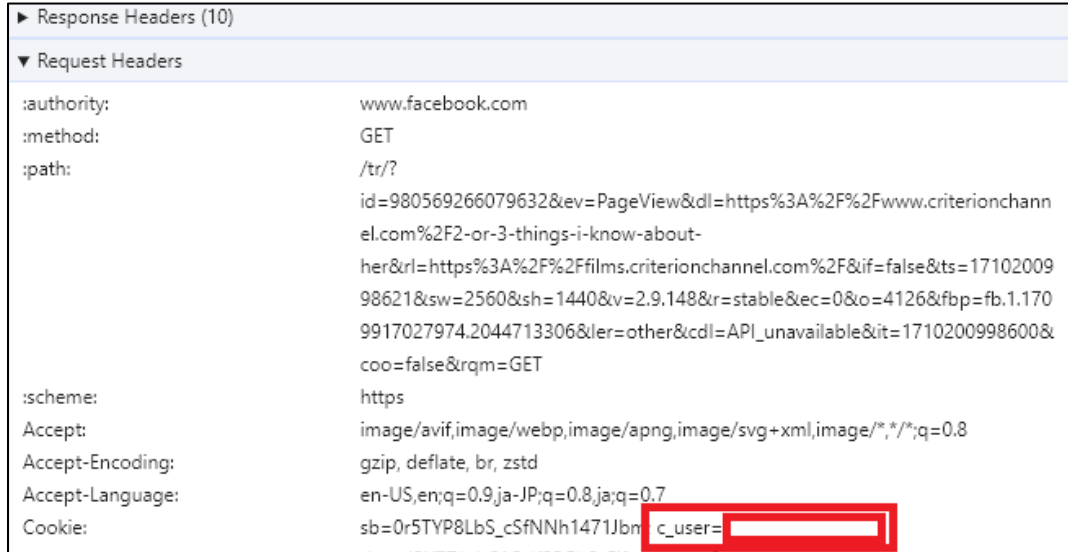
61. A c_user cookie is a unique identifier that singles out an individual Meta profile. The string of numbers is unique to every Meta account—distinguishing each FBID from its peers.

62. Any person, even without in-depth technical expertise, can utilize the FBID to identify owners of the FBID via their Facebook profile. Once the Meta Pixel’s routine exchange of information is complete, the FBID that becomes available can be used by any individual of ordinary skill and technical proficiency to easily identify a Facebook user, by simply appending the Facebook FBID to www.facebook.com (www.facebook.com/[UID_here]). That step, readily available through any internet browser, will direct the browser to the profile page, and all the information contained in or associated with the profile page, for the user associated with the particular FBID.

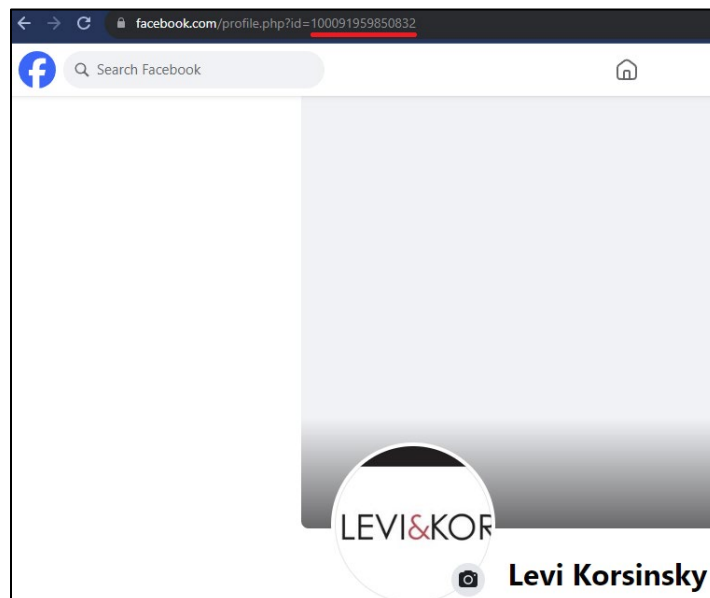
²⁰ *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 290 (3d Cir. 2016).

²¹ See *Lebakken v. WebMD, LLC* 2022 U.S. Dist. LEXIS 201010, at *11-12 (N.D. Ga. Nov. 4, 2022); *Czarnionka v. Epoch Times Ass’n*, 2022 U.S. Dist. LEXIS 209067, at *8-10 (S.D.N.Y. Nov. 17, 2022); *Ambrose v. Boston Globe Media Partners, LLC*, 2022 U.S. Dist. LEXIS 168403, at *5-6 (D. Mass. Sept. 19, 2022).

63. The following screenshot of the captured network traffic shows Defendant disclosing a Website user's Meta ID to Meta through the Pixel when the user views a video on the Website (the Meta ID is redacted for privacy reasons):



64. An ordinary person can identify a user using a Meta ID. Levi & Korsinsky created a generic test Meta account to investigate the functionality of the Pixel. This test FBID is “100091959850832.” And appending the test FBID to the Meta URL in a standard internet browser (here becoming www.facebook.com/100091959850832) will redirect the browser straight to the Meta profile associated with the FBID, as depicted in the screenshot, below:



65. Importantly, some Facebook profile information—name, gender, profile photo, cover photo, username, Meta ID, age range, language, and country—are “always public.”²² No privacy setting on Facebook would allow Website users, or any user, to hide this basic information.

F. Defendant Discloses Subscribers’ Video-Viewing Information to Twilio and Meta

66. As the dynamic analysis established, Defendant discloses to Twilio, through Segment, the full title of the pre-recorded video watched by Website and App users, in the form of parameters and metadata containing the plain title of the video and/or the Universal Resource Locator (“URL”) of the video. On the App, Defendant also discloses to Twilio interactions associated with the video, such as whether the video was played:

//

//

//

//

//

//

//

//

//

//

//

//

²² CONTROL WHO CAN SEE WHAT YOU SHARE ON FACEBOOK, FACEBOOK, <https://www.facebook.com/help/1297502253597210>.

```

user_id: 64513575
video_id: 3269060
view: video
session_id: 895aa9bb2fe1b023ae5985bc19353652
collection title: Heisei-Era Godzilla
video_title: Godzilla vs. Biollante
name: video
name: The Criterion Channel
version: None
externalIds: {'collection': 'users', 'encoding': 'none', 'type': 'vimeo_id', 'id': '64513575'}
locale: en-US
timezone: America/New_York
name: Penelope Strickland
email: blimalamamama@gmail.com
vimeo_id: 64513575
path: /heisei-era-godzilla/season:1/videos/godzilla-vs-biollante
referrer: https://www.criterionchannel.com/heisei-era-godzilla
search:
title: Godzilla vs. Biollante - Heisei-Era Godzilla - The Criterion Channel
url: https://www.criterionchannel.com/heisei-era-godzilla/season:1/videos/godzilla-vs-biollante

```

Defendant's Disclosure of the Title of the Pre-Recorded Videos Watched By Website Users to Twilio

```

"duration": "6296",
"is_airplay": "0",
"is_chromecast": "0",
"is_drm": "1",
"is_fullscreen": "0",
"is_live": "0",
"is_trailer": "0",
"name": "Video Playback Paused",
platform": "iphone",
platform_id": "3447",
platform_version": "v8.800.1",
product_id": "39621",
session_id": "QM90ZD6F-0196-KA9Y-NK7G-ZSNIUGBHX0JH",
site_id": "59054",
timecode": "122",
timestamp": "1721651494",
type": "video",
user_email": "peppymay@yahoo.com",
user_id": "64533512",
video_id": "3269060",
video_title": "Godzilla vs. Biollante"
},

```

Defendant's Disclosure of the Title of the Pre-Recorded Videos Watched and Video Interactions By App Users to Twilio (iOS)

```

"duration": "8008.0",
"is_airplay": "0.0",
"is_chromecast": "0.0",
"is_drm": "1.0",
"is_fullscreen": "1.0",
"is_live": "0.0",
"is_trailer": "0.0",
"name": "Video Playback Buffer Started",
platform": "android",
platform_id": "3449.0",
platform_version": "v8.703.1",
session_id": "3ab79ae5-c910-4714-ab9b-eff7992cf69f",
site_id": "59054.0",
timecode": "0.0",
timestamp": "1.723482093E9",
type": "video",
user_email": "lari.shirokaka@gmail.com",
user_id": "61091066",
video_id": "3308698.0",
video_title": "Licorice Pizza"
},

```

Defendant's Disclosure of the Title of the Pre-Recorded Videos Watched and Video Interactions By App Users to Twilio (Android)

67. Even outside of the video title, an ordinary person can identify the video from the disclosed URL. For example, the following Google search shows the disclosed URL. If searched while signed into an existing Criterion Channel account, the URL would have taken even an ordinary person directly to the watched video:



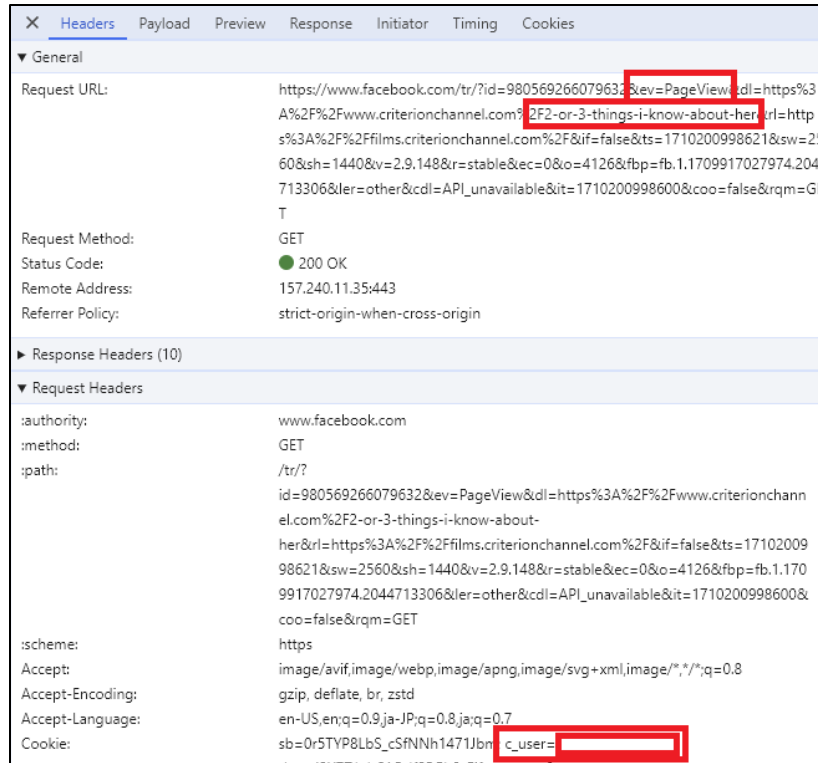
68. The dynamic analysis also shows that Defendant discloses the URL (and thereby the video's full title) of the pre-recorded video requested or obtained by Website users watched videos to Meta. This occurs if the Website users also have a Meta account that they were signed into at the time of requesting or obtaining the pre-recorded video on Defendant's Website:

//

//

//

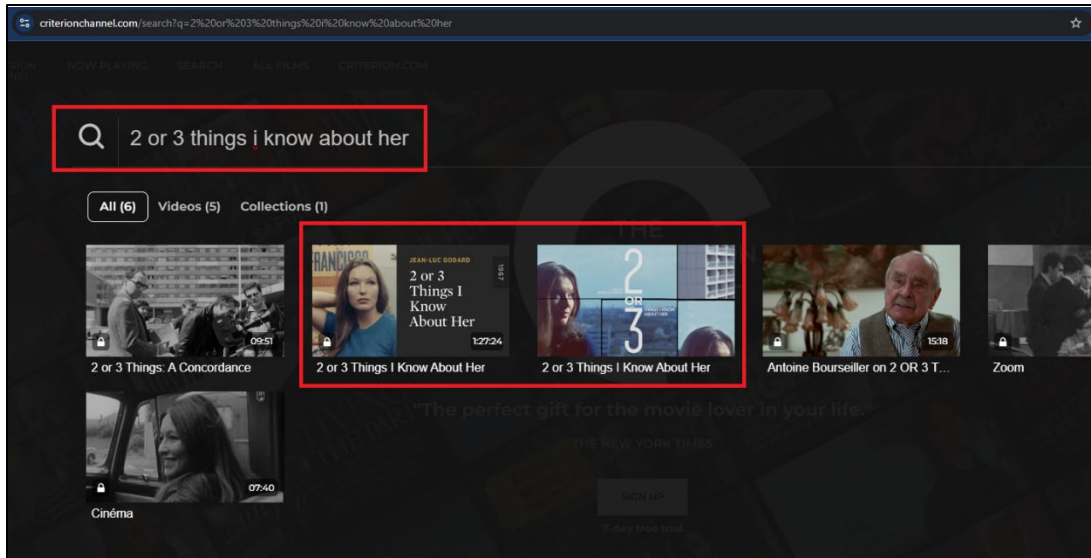
//



69. As shown in the excerpted network request above, Defendant discloses the full title of a video that a Website user has requested or obtained to Meta through the Pixel. In the above example, the user requested the video “2 or 3 Things I Know About Her,” the full title of which is disclosed in the “Request URL.”

70. This video can be easily located by even an ordinary person. The following screenshot shows a search of the disclosed video title, “2 or 3 Things I Know About Her,” on Defendant’s Website:²³

²³ *2 or 3 Things I Know About Her*, CRITERION CHANNEL, www.criterionchannel.com/2-or-3-things-i-know-about-her.



IV. DEFENDANT DISCLOSES SUBSCRIBERS' PII TO THIRD PARTIES FOR THE PURPOSES OF MARKETING, ADVERTISING, AND ANALYTICS

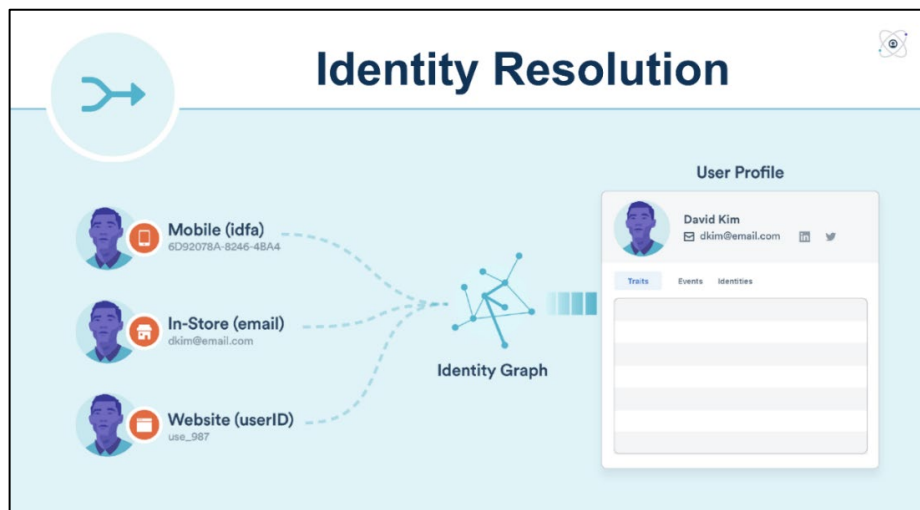
A. Defendant Discloses Subscribers' PII To Twilio For Marketing, Advertising, And Analytics

71. Defendant transmits its users' PII to Twilio so that Defendant can analyze user data, launch marketing campaigns, and target specific users or specific groups of users for advertisements. All of this, especially in conjunction with Segment's marketing and advertising services, helps Defendant monetize the Criterion Channel Service and maximize revenue by collecting and disclosing as much PII as possible to Twilio via Segment.

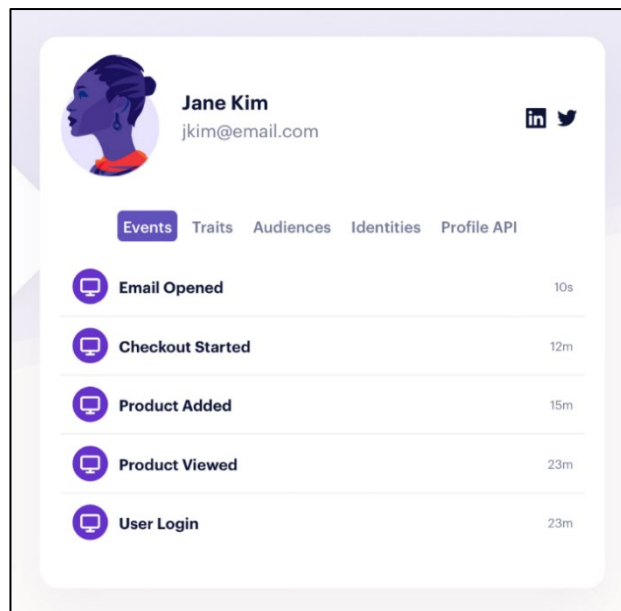
72. Twilio entices developers to integrate Segment by underscoring its signature feature: "Engage." Engage "uses Segment Identity Resolution to take event data from across devices and channels and intelligently merge it into complete user- or account-level profiles."²⁴ This allows Twilio and Defendant to "understand a user's interaction across web, mobile, server, and third-party partner touch-points in real time, using an online and offline ID graph with support

²⁴ ENGAGE INTRODUCTION, SEGMENT, <https://segment.com/docs/engage/>.

for cookie IDs, device IDs, emails, and custom external IDs,” which are all “matched to one persistent ID”²⁵:



73. Once Twilio has built these comprehensive user profiles for Defendant, Twilio can then “group customers based on commonly used methods: demographic, psychographic, and geographic”²⁶:



²⁵ IDENTITY RESOLUTION OVERVIEW, SEGMENT, <https://segment.com/docs/unify/identity-resolution/>.

²⁶ CUSTOMER SEGMENTATION TOOLS | SEGMENT, <https://segment.com/growth-center/customer-segmentation/tools-software/>.

74. Twilio leverages these profiles to help website operators and/or app developers, like Defendant “[p]ower personalized marketing campaigns”²⁷ directed at Engage profiles that fit specific parameters. Defendant does this through Twilio’s “Audience” feature, which “let[s] you group users or accounts based on event behavior and traits that Segment tracks.”²⁸

75. Twilio also enables Defendant to conduct targeted marketing by “integrat[ing] websites & mobile apps data to over 300 analytics and growth tools,”²⁹ which Twilio calls “Destinations.”³⁰ Segment’s Destinations are used for, *inter alia*, “Advertising”; “Analytics”; “Attribution”; “Enrichment”; “Marketing Automation”; “Performance Monitoring”; and/or “Personalization”³¹—in short, “to personalize messages across channels[and] optimize ad spend.”³² For instance, Twilio helps developers “run advertising campaigns without having to manually update the list of users to target”³³ by sending data to the Google Ads Remarketing Lists destination. Defendant uses Twilio for such marketing purposes.

76. Defendant also discloses users’ PII to Twilio so it can better target advertisements. After Defendant discloses users’ PII, Twilio compiles and transmits that information to other third

²⁷ SEGMENT, PROFILE API, <https://segment.com/docs/unify/profile-api/>.

²⁸ ENGAGE AUDIENCE OVERVIEW, SEGMENT, <https://segment.com/docs/engage/audiences/>.

²⁹ SEGMENT, HOW SEGMENT WORKS, <https://segment.com/docs/getting-started/01-what-is-segment/>.

³⁰ SEGMENT, AN INTRODUCTION TO SEGMENT, <https://segment.com/docs/guides/> (last accessed Apr. 30, 2024).

³¹ SEGMENT, DESTINATION CATALOG, <https://segment.com/docs/connections/destinations/catalog/>. *See also* SEGMENT, DESTINATION LIST, <https://segment.com/docs/connections/destinations/catalog/index-all/>.

³² SEGMENT, USING YOUR ENGAGE DATA, <https://segment.com/docs/personas/using-personas-data/>.

³³ SEGMENT, GOOGLE ADS REMARKETING LISTS DESTINATION, <https://segment.com/docs/connections/destinations/catalog/adwords-remarketing-lists/>.

parties “to personalize messages across channels, optimize ad spend, and improve targeting.”³⁴ These third parties include Facebook, Google, and Salesforce.³⁵

77. Defendant also discloses users’ PII to Twilio so it can better measure and analyze the Criterion Channel Service’s performance. Defendant does this by leveraging Twilio’s “Audiences” feature, which breaks down user profiles into a number of traits, like “total minutes watched.”³⁶

B. Defendant Discloses Subscribers’ PII To Meta For Marketing, Advertising, And Analytics

78. Defendant discloses Website users’ Meta ID and video-viewing activity to Meta so that Meta can “personali[ze] content, tailor[] and measur[e] ads, and provid[e] a safer experience” for Website users.³⁷

79. The Meta Tracking Pixel allows Defendant “to track [their] website visitors’ actions,” which Meta calls conversion tracking.³⁸ “Tracked conversions ... can be used to analyze [Defendant’s] return on ad investment.”³⁹

80. Notably, “[e]ach time the Pixel loads, it automatically ... track[s]” and records the URL that a Website user viewed.⁴⁰ In other words, so long as Defendant has installed the Meta

³⁴ USING YOUR ENGAGE DATA, SEGMENT, <https://segment.com/docs/personas/using-personas-data/>.

³⁵ *Id.*

³⁶ COMPUTED TRAITS, SEGMENT, <https://segment.com/docs/unify/traits/computed-traits/>.

³⁷ COOKIES POLICY, META, https://www.facebook.com/privacy/policies/cookies/?entry_point=cookie_policy_redirect&entry=0.

³⁸ CONVERSION TRACKING, META, <https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking>.

³⁹ *Id.*

⁴⁰ CUSTOM CONVERSIONS, META, <https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking#custom-conversions>.

Tracking Pixel onto the Website, anyone who views that webpage—meaning all Website users—“will be tracked using that” automatic URL tracker.⁴¹ And, as mentioned above, the tracked URL discloses to Meta the exact video(s) that a Website user views.

81. Indeed, Meta even warns advertisers such as Defendant to “make sure” the Website URLs are specific enough that Defendant “can define visitor actions exclusively based on unique ... website URLs.”⁴²

82. “Once tracked, custom conversions”—such as the URL tracking tool—“can be used to optimize [Defendant’s] ad campaigns”⁴³ through other Meta tools such as Ads Insights.⁴⁴

83. Defendant utilizes Meta’s comprehensive array of tracking tools to optimize their marketing, advertising, and analytics—ultimately increasing their viewer base and revenue.

V. DEFENDANT KNOWINGLY DISCLOSES SUBSCRIBERS’ PII TO TWILIO AND META

84. Based on the above, it is abundantly clear that Defendant *intentionally* and *knowingly* discloses its subscribers’ PII to Twilio and Meta.

85. As outlined above, Defendant “knew that it was collecting data from users that identified personalized information about them because, in exchange for the data, [Twilio] provided [Defendant] with analytics allowing it to provide advertisements tailored to specific users.” *Saunders v. Hearst Television, Inc.*, 711 F. Supp. 3d 24, 31 (D. Mass. 2024).

86. Defendant also knowingly and intentionally installed and set up the Meta Pixel to collect subscriber data. To activate and employ a Meta Pixel, a website owner must first sign up

⁴¹ *Id.*

⁴² *Id.*

⁴³ *Id.*

⁴⁴ CUSTOM CONVERSIONS INSIGHTS, META, <https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking#custom-conversions>.

for a Meta account, where specific “business manager” accounts are provided the most utility for using the Pixel.⁴⁵ To add an operational Pixel to a website, the website owner or operator must take several affirmative steps, including naming the Pixel during the creation and setup of the Pixel.⁴⁶

87. Once the Pixel is created, the website operator assigns access to the Pixel to specific people for management purposes,⁴⁷ and must connect the Pixel to a Facebook Ad account.⁴⁸ A Pixel cannot be placed on a website by a third-party. It must be placed directly by or on behalf of the OTT service owner.

88. Only after the Pixel is set and activated can it begin collecting, sharing, and using Subscribers’ personally identifying information and activity as instructed by the website owner.

89. Defendant had and continues to have the choice to design the Criterion Channel Service to determine which third parties it integrates into the Website and/or App, and what information is disclosed to those third parties. Nonetheless, Defendant has chosen to integrate Twilio and Meta in such a way that it discloses extensive PII to each to maximize its revenue from marketing and advertising efforts.

90. Moreover, common sense dictates that a sophisticated media industry participant like Defendant—who integrated Segment and the Meta Pixel precisely for their marketing,

⁴⁵ BUSINESS HELP CENTER: HOW TO CREATE A META PIXEL IN BUSINESS MANAGER, FACEBOOK, <https://www.facebook.com/business/help/314143995668266?id=1205376682832142>.

⁴⁶ *Id.*; see also Ivan Mana, *How to Set Up & Install the Facebook Pixel (In 2022)*, YOUTUBE, available at <https://www.youtube.com/watch?v=ynTNs5FAUm8>.

⁴⁷ BUSINESS HELP CENTER: ADD PEOPLE TO YOUR META PIXEL IN YOUR META BUSINESS MANAGER, FACEBOOK <https://www.facebook.com/business/help/279059996069252?id=2042840805783715>.

⁴⁸ *Business Help Center: Add An Ad Account To A Meta Pixel In Meta Business Manager*, FACEBOOK, <https://www.facebook.com/business/help/622772416185967>.

advertising, and analytics capabilities—is fully aware of the scope of the data that these Third Parties collect. Indeed, Defendant would need to contract with Twilio and Meta specifically for their marketing, advertising, and analytics services, in order for the technologies here at issue to be implemented into the Criterion Channel Service.

91. Further, Defendant is more than capable of observing what information is disclosed to each of these third parties through publicly available software like Charles Proxy.⁴⁹

92. Therefore, Defendant knowingly and intentionally provides personal information and video-viewing information to Segment and Meta for marketing, advertising, and analytics services.

VI. EXPERIENCES OF PLAINTIFFS

A. Plaintiff Francis Lucchese-Soto

93. In or around June 2022, Plaintiff Francis Lucchese-Soto created an account and purchased a subscription to The Criterion Channel Service. From June 2022 through 2024, Plaintiff Soto regularly watched pre-recorded videos on the Criterion Channel iOS App on his Apple iPad while signed into his Criterion Channel Service account, including video content only available to subscribers.

94. Plaintiff Soto provided Defendant with his name, e-mail address, and credit card information as part of signing up for the Criterion Channel Service.

95. At all relevant times, Plaintiff Soto never consented to, agreed to, or otherwise permitted Defendant’s disclosure of his PII to third parties, including Twilio. Likewise, Defendant never gave Plaintiff Soto the opportunity to prevent the disclosure of his PII to third parties, including Twilio.

⁴⁹ CHARLES WEB DEBUGGING PROXY APPLICATION, <https://www.charlesproxy.com/>.

96. Nevertheless, each time Plaintiff Soto viewed a pre-recorded video on the Criterion Channel App, Defendant disclosed Plaintiff Soto's PII to Twilio. Specifically, Defendant disclosed Plaintiff Soto's: (i) name, (ii) e-mail address, (iii) user ID, and (iv) the title of the pre-recorded video viewed by Plaintiff Soto, and (v) video interactions, including as the fact that Plaintiff Soto actually viewed the video.

97. Using this information, Twilio was able to identify Plaintiff Soto and attribute his video viewing records to an individualized profile of Plaintiff Soto. Indeed, even an ordinary person could identify Plaintiff Soto using the information Defendant disclosed to Twilio. Twilio compiled Plaintiff Soto's PII and video-viewing activity on The Criterion Channel App, which Defendant used and continues to use for marketing, advertising, and analytics purposes.

B. Plaintiff Kevin McGuire

98. In or around 2018, Plaintiff McGuire created an account and purchased a subscription to The Criterion Channel. From 2018 through today, Plaintiff McGuire used his Chrome internet browser to watch pre-recorded videos on the Website, including video content only available to subscribers, while signed into his Criterion Channel Service account and Meta account. Plaintiff McGuire was in Pennsylvania when he viewed each of these videos.

99. Plaintiff McGuire provided Defendant with his name, e-mail address, and credit card information as part of signing up for the Criterion Channel Service. Plaintiff McGuire had his full name, a picture of himself, his profession, his location, his hometown, his high school, his college and his college major, and his marital status all on his public Facebook profile page.

100. At all relevant times, Plaintiff McGuire never consented to, agreed to, or otherwise permitted Defendant's disclosure of his PII to third parties, including Twilio and Meta. Likewise, Defendant never gave Plaintiff McGuire the opportunity to prevent the disclosure of his PII to third parties, including Twilio and Meta.

101. Nevertheless, each time Plaintiff McGuire viewed a pre-recorded video on the Criterion Channel Website, Defendant disclosed Plaintiff McGuire's PII to Twilio and Meta. Specifically, as to Twilio, Defendant disclosed Plaintiff McGuire's: (i) name, (ii) e-mail address, (iii) user ID, and (iv) the title of the pre-recorded video viewed by Plaintiff McGuire.

102. Likewise, as to Meta, Defendant disclosed Plaintiff McGuire's: (i) c_user cookie (Meta ID); and (ii) the URL of the pre-recorded video Plaintiff McGuire watched, which includes the full title of the video.

103. Using this information, Twilio and Meta were able to identify Plaintiff McGuire and attribute his video viewing records to an individualized profile of Plaintiff McGuire. Indeed, even an ordinary person could identify Plaintiff McGuire using the information Defendant disclosed to the Third Parties. The Third Parties compiled Plaintiff McGuire's PII and video-viewing activity on The Criterion Channel Website, which Defendant used and continues to use for marketing, advertising, and analytics purposes.

C. Plaintiff Matthew Wickham

104. In or around 2018, Plaintiff Wickham created an account and purchased a subscription to The Criterion Channel. From 2018 through today, Plaintiff Wickham used his Chrome internet browser to watch pre-recorded videos on the Website, including video content only available to subscribers, while signed into his Criterion Channel Service account and Meta account. Plaintiff Wickham was in Florida when he viewed each of these videos.

105. Plaintiff Wickham provided Defendant with his name, e-mail address, and credit card information as part of signing up for the Criterion Channel Service. Plaintiff Wickham had his full name and location on his public Facebook profile page.

106. At all relevant times, Plaintiff Wickham never consented to, agreed to, or otherwise permitted Defendant's disclosure of his PII to third parties, including Twilio and Meta. Likewise,

Defendant never gave Plaintiff Wickham the opportunity to prevent the disclosure of his PII to third parties, including Twilio and Meta.

107. Nevertheless, each time Plaintiff Wickham viewed a pre-recorded video on the Criterion Channel Website, Defendant disclosed Plaintiff Wickham's PII to Twilio and Meta. Specifically, as to Twilio, Defendant disclosed Plaintiff Wickham's: (i) name, (ii) e-mail address, (iii) user ID, and (iv) the title of the pre-recorded video viewed by Plaintiff Wickham.

108. Likewise, as to Meta, Defendant disclosed Plaintiff Wickham's: (i) c_user cookie (Meta ID); and (ii) the URL of the pre-recorded video Plaintiff Wickham watched, which includes the full title of the video.

109. Using this information, Twilio and Meta were able to identify Plaintiff Wickham and attribute his video viewing records to an individualized profile of Plaintiff Wickham. Indeed, even an ordinary person could identify Plaintiff Wickham using the information Defendant disclosed to the Third Parties. The Third Parties compiled Plaintiff Wickham's PII and video-viewing activity on The Criterion Channel Website, which Defendant used and continues to use for marketing, advertising, and analytics purposes.

D. Plaintiff Amitai Heller

110. In or around 2023, Plaintiff Heller created an account and purchased a subscription to The Criterion Channel. From 2023 through 2024 Plaintiff Heller used his Chrome internet browser to watch pre-recorded videos on the Website, including video content only available to subscribers, while signed into his Criterion Channel Service account and Meta account.

111. Plaintiff Heller provided Defendant with his name, e-mail address, and credit card information as part of signing up for the Criterion Channel Service. Plaintiff Heller had his name and picture on his public Facebook profile page.

112. At all relevant times, Plaintiff Heller never consented to, agreed to, or otherwise

permitted Defendant's disclosure of his PII to third parties, including Twilio and Meta. Likewise, Defendant never gave Plaintiff Heller the opportunity to prevent the disclosure of his PII to third parties, including Twilio and Meta.

113. Nevertheless, each time Plaintiff Heller viewed a pre-recorded video on the Criterion Channel Website, Defendant disclosed Plaintiff Heller's PII to Twilio and Meta. Specifically, as to Twilio, Defendant disclosed Plaintiff Heller's: (i) name, (ii) e-mail address, (iii) user ID, and (iv) the title of the pre-recorded video viewed by Plaintiff Heller.

114. Likewise, as to Meta, Defendant disclosed Plaintiff Heller's: (i) c_user cookie (Meta ID); and (ii) the URL of the pre-recorded video Plaintiff Heller watched, which includes the full title of the video.

115. Using this information, Twilio and Meta were able to identify Plaintiff Heller and attribute his video viewing records to an individualized profile of Plaintiff Heller. Indeed, even an ordinary person could identify Plaintiff Heller using the information Defendant disclosed to the Third Parties. The Third Parties compiled Plaintiff Heller's PII and video-viewing activity on The Criterion Channel Website, which Defendant used and continues to use for marketing, advertising, and analytics purposes.

THE PARTIES

116. Plaintiff Francis Lucchese-Soto is, and has been at all relevant times, a citizen of Illinois who resides in Arlington Heights, Illinois.

117. Plaintiff Kevin McGuire is, and has been at all relevant times, a citizen of Pennsylvania who resides in Pittsburgh, Pennsylvania.

118. Plaintiff Matthew Wickham is, and has been at all relevant times, a citizen of Florida who resides in Vero Beach, Florida.

119. Plaintiff Amitai Heller is, and has been at all relevant times, a citizen of Oregon who resides in Portland, Oregon.

120. Defendant The Criterion Collection, LLC is a Delaware limited liability company with its principal place of business at 215 Park Ave S., New York, New York 10003. Defendant develops, owns, and operates the Criterion Channel Service, which is available throughout the United States.

JURISDICTION AND VENUE

121. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because it arises under a law of the United States (the VPPA and the Federal Wiretap Act).

122. This Court also has subject matter jurisdiction over this civil action pursuant to 28 U.S.C. § 1332(d) because there are more than 100 class members, the aggregate amount in controversy exceeds \$5,000,000, exclusive of interest, fees, and costs, and at least one Class member is a citizen of a state different from Defendant.

123. Defendant is an “unincorporated association” under the Class Action Fairness Act (“CAFA”), 28 U.S.C. § 1332(d), and Defendant is therefore “a citizen of the State where it has its principal place of business [New York] and the State under whose laws it is organized [Delaware].” *See* 28 U.S.C. § 1332(d)(10).

124. This Court has personal jurisdiction over Defendant because it is headquartered in New York.

125. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant resides in this District.

CLASS ALLEGATIONS

126. **Class Definition:** Plaintiffs seek to represent a class of similarly situated

individuals defined as all persons in the United States who subscribed to the Criterion Channel Service (either the Website or App), used the Criterion Channel Service to watch pre-recorded videos, and had their PII disclosed to a third party (the “Class”).

127. **Meta Subclass Definition:** Plaintiffs McGuire, Wickham, and Heller seek to represent a subclass of similarly situated individuals defined as all persons in the United States who subscribed to the Criterion Channel Service (either the Website or App), used the Criterion Channel Service to watch pre-recorded videos while signed into their Meta account, and had their PII disclosed to Meta (the “Meta Subclass”).

128. **Pennsylvania Subclass Definition:** Plaintiff McGuire seeks to represent a subclass of similarly situated individuals defined as all Pennsylvania residents who subscribed to the Criterion Channel Service (either the Website or App), used the Criterion Channel Service to watch pre-recorded videos while in Pennsylvania, and had their PII disclosed to a third party (the “Pennsylvania Subclass”).

129. **Florida Subclass Definition:** Plaintiff Wickham seeks to represent a subclass of similarly situated individuals defined as all Florida residents who subscribed to the Criterion Channel Service (either the Website or App), used the Criterion Channel Service to watch pre-recorded videos while in Florida, and had their PII disclosed to a third party (the “Florida Subclass”).

130. The Class, the Meta Subclass, the Pennsylvania Subclass, and the Florida Subclass shall be collectively referred to as the “Classes.”

131. Subject to additional information obtained through further investigation and discovery, the above-described Classes may be modified or narrowed as appropriate, including through the use of multi-state subclasses.

132. **Numerosity (Fed. R. Civ. P. 23(a)(1)):** At this time, Plaintiffs do not know the exact number of members of the Classes. However, given the popularity of the Criterion Channel, the number of persons within the Classes is believed to be in the hundreds of thousands and therefore so numerous that joinder of all members is impractical.

133. **Commonality and Predominance (Fed. R. Civ. P. 23(a)(2), 23(b)(3)):** There is a well-defined community of interest in the questions of law and fact involved in this case. Questions of law and fact common to the members of the Classes that predominate over questions that may affect individual members of the Classes include:

- (a) whether Defendant unlawfully disclosed and continues to disclose Criterion Channel Service users' PII, in violation of the VPPA, the Federal Wiretapping Act, the WESCA, and the FSCA;
- (b) whether Defendant's disclosures were committed intentionally or knowingly; and
- (c) whether Defendant disclosed Plaintiffs' and members of the Class' PII without consent.

134. **Typicality (Fed. R. Civ. P. 23(a)(3)):** Plaintiffs' claims are typical of those of the Classes because Plaintiffs, like all members of the Classes, watched pre-recorded videos on the Criterion Channel Service and had their PII disclosed to third parties, such as Twilio and Meta.

135. **Adequacy (Fed. R. Civ. P. 23(a)(4)):** Plaintiffs have retained and are represented by qualified and competent counsel who are highly experienced in complex consumer class action litigation, including litigation concerning the VPPA, the Federal Wiretapping Act, and their state-inspired offspring. Plaintiffs and their counsel are committed to vigorously prosecuting this class action. Moreover, Plaintiffs can fairly and adequately represent and protect the interests of the Classes. Neither Plaintiffs nor their counsel have any interest adverse to, or in conflict with, the interests of the absent members of the Classes. Plaintiffs have raised viable statutory claims, of

the type reasonably expected to be raised by members of the Classes, and Plaintiffs will vigorously pursue those claims. If necessary, Plaintiffs may seek leave of this Court to amend this Complaint to include additional representatives to represent the Classes, additional claims as may be appropriate, or to amend the definition of the Classes to address any steps that Defendant takes.

136. **Superiority (Fed. R. Civ. P. 23(b)(3)):** A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of the claims of all members of the Classes is impracticable. Even if every member of the Classes could afford to pursue individual litigation, the court system could not. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed. Individualized litigation would also present the potential for varying, inconsistent or contradictory judgments, and would magnify the delay and expense to all parties and to the court system resulting from multiple trials of the same factual issues. By contrast, the maintenance of this action as a class action, with respect to some or all of the issues presented herein, presents few management difficulties, conserves the resources of the parties and of the court system and protects the rights of each member of the Classes. Plaintiffs anticipate no difficulty in the management of this action as a class action.

CAUSES OF ACTION

COUNT I

Violation Of The Video Privacy Protection Act, 18 U.S.C. § 2710

137. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

138. Plaintiffs bring this claim individually and on behalf of the members of the Classes against Defendant.

139. 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 Defendant provides video (*i.e.*, “similar audio visual materials” under the VPPA’s definition) to consumers via the Criterion Channel Service.

140. Plaintiffs and members of the Classes are “consumers” as defined by the VPPA because they purchased a subscription to the Criterion Channel Service and created a Criterion Channel Service Account, through which they provided their PII to Defendant, and Plaintiffs and members of the Classes were granted access to Defendant’s library of video content in return. *See* 18 U.S.C. § 2710(a)(1); *see also Salazar*, 118 F.4th at 550-53.

141. Plaintiffs and members of the Classes viewed pre-recorded videos using the Criterion Channel Service. During these occasions, and as set forth above, Defendant disclosed Plaintiffs’ and members of the Classes’ PII to third parties, including Twilio and Meta. The information disclosed by Defendant constitutes “personally identifiable information” because it enables even an ordinary person to identify which specific videos were watched by which specific Plaintiffs and which specific members of the Classes. 18 U.S.C. § 2710(a)(3).

142. Defendant’s disclosures of Plaintiffs’ and members of the Classes’ PII to Twilio and Meta constitute “knowing[] disclosures” of Plaintiffs’ and members of the Classes’ “personally identifiable information” to a person as proscribed by the VPPA. 18 U.S.C. § 2710(a)(1).

143. Plaintiffs and Class members did not provide Defendant with any form of consent—either written or otherwise—to disclose their PII to third parties, including Twilio and Meta. Nor were Defendant’s disclosures made in the “ordinary course of business” as the term is defined by the VPPA. In particular, Defendant’s disclosures to Twilio and Meta were not

necessary for “debt collection activities, order fulfillment, request processing, [or] transfer of ownership.” 18 U.S.C. § 2710(a)(2).

144. On behalf of themselves and the Classes, Plaintiffs seek: (i) declaratory relief; (ii) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs 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 and costs and other litigation expenses.

COUNT II
Violation Of The Federal Wiretap Act,
18 U.S.C. §§ 2510, *et seq.*

145. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

146. Plaintiffs bring this claim individually and on behalf of the members of the Classes against Defendant.

147. The Federal Wiretap Act prohibits the interception, use, and disclosure of any electronic communications without the consent of at least one authorized party to the communication. 18 U.S.C. §§ 2511(1)(a)-(e). The Federal Wiretap Act also prohibits a person from “procur[ing] any other person” to intercept any electronic communications. 18 U.S.C. § 2511(a)(a).

148. The Federal Wiretap Act confers a civil private right of action to “any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter.” 18 U.S.C. § 2520(a).

149. The Federal Wiretap Act defines “intercept” 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.” 18 U.S.C. § 2510(4).

150. The Federal Wiretap Act defines “contents” as “includ[ing] any information concerning the substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(8).

151. The Wiretap Act defines “person” as “any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation.” 18 U.S.C. § 2510(6).

152. The Wiretap Act defines “electronic communication” as “any 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 that affects interstate or foreign commerce.” 18 U.S.C. § 2510(12).

153. Defendant and the Third Parties are “persons” for the purposes of the Wiretap Act. Segment and the Meta Pixel each constitute a “device or apparatus which can be used to intercept a wire, oral, or electronic communication.” 18 U.S.C. § 2510(5).

154. The communications that Plaintiffs and members of the Classes had with the Criterion Channel Service, in the form of their PII were intercepted by the Third Parties. Such communications are “electronic communications” under 18 U.S.C. § 2510(12).

155. Plaintiffs and members of the Classes had a reasonable expectation of privacy in their electronic communications with the Criterion Channel Service. Not only do Plaintiffs and members of the Classes have a reasonable expectation of privacy in their PII (such as full names, e-mail addresses, and Meta IDs), Congress has declared that consumers have a right to the privacy of their video-viewing information, as such information is “a window into our loves, likes, and dislikes.” S. Rep. No. 100-599 at 6-7 (1988) (remarks by Senator Paul Simon).

156. Plaintiffs and members of the Classes reasonably expected that no third parties were intercepting, recording, or otherwise receiving their electronic communications with the Criterion Channel Service.

157. Nonetheless, Defendant secretly procured and used Twilio and the Meta Pixel provided by the Third Parties to intercept Plaintiffs' and members of the Classes' communications with the Criterion Channel Service without Plaintiffs' and members of the Classes' consent.

158. Defendant's conduct was knowing, willful, and intentional, as Defendant is a sophisticated party with full knowledge of the functionality of the Third Parties whose services it was procuring, using, and integrating on the Criterion Channel Service. In addition, Defendant knowingly, willfully, and intentionally oversaw the integration, installation, and use of Segment and the Meta Pixel on the Website, and Segment on the App, such that Defendant caused the private communications between itself and its users to be shared with third parties.

159. Plaintiffs and members of the Classes never consented to expose their confidential electronic communications with the Criterion Channel Service to third parties. Indeed, such consent could not have been given as Defendant never sought any form of consent from Plaintiffs and members of the Classes to intercept, record, and disclose their private communications with the Criterion Channel Service.

160. As detailed above, the Third Parties' unauthorized interception, disclosure, and use of Plaintiffs' confidential communications were only possible through Defendant's knowing, willful, or intentional implementation of the Third Parties' services into Defendant's Criterion Channel Website and App. 18 U.S. Code § 2511(1)(a).

161. Plaintiffs and Class members have been damaged due to the unauthorized interception, disclosure, and use of their confidential communications in violation of 18 U.S.C. § 2520. As such, Plaintiffs and Class members are entitled to: (i) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiffs and any profits made by the Third Parties as a result of the violation, or (b) statutory damages of whichever is the greater of \$100 per day per violation or \$10,000; (ii) appropriate equitable or declaratory relief; and (iii) reasonable attorneys' fees and other costs reasonably incurred.

COUNT III

Violation Of The Pennsylvania Wiretapping And Electronic Surveillance Control Act, 18 Pa. Cons. Stat. §§ 5701, *et seq.*

162. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

163. Plaintiff McGuire brings this claim individually and on behalf of the members of the proposed Pennsylvania Subclass against Defendant.

164. The WESCA prohibits any person from willfully intercepting, endeavoring to intercept, or procuring of any other person to intercept or endeavor to intercept, any wire, electronic, or oral communication. 18 Pa. Cons. Stat. §§ 5701, 5703(1).

165. Defendant and each of the Third Parties are “persons” as defined by 18 Pa. Cons. Stat. § 5702.

166. Defendant procured the Third Parties to “intercept” Plaintiff McGuire’s and Pennsylvania Subclass members’ communications with the Criterion Channel Service. The WESCA defines “intercept” as “[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device.” 18 Pa. Cons. Stat. § 5702.

167. Defendant subsequently used the contents of Plaintiff McGuire’s communications with the Criterion Channel Service, intercepted and processed by the Third Parties, to unlawfully target users with marketing and advertising. 18 Pa. Cons. Stat. §§ 5703(2)-(3).

168. The WESCA also prohibits the knowing attempt to retrieve a wire or electronic communication while said communication is in electronic storage. Accordingly, Defendant is prohibited from intentionally accessing or exceeding the scope of access to a facility through which an electronic communication service is provided in order to retrieve a wire or electronic communication. 18 Pa. Cons. Stat. § 5741(a)(1)-(2).

169. In violation of the WESCA, Defendant procured, obtained, and integrated the Third Parties’ services (Segment and the Meta Pixel) into the Criterion Channel Service to intercept and/or improperly access the communications between Defendant and its Subscribers during the conduct of its business.

170. Segment and the Meta Pixel constitute “electronic ... devices” or “apparatuses” as defined by 18 Pa. Cons. Stat. § 5702. Notwithstanding such software qualifies on its own, for such “software to work, it must be run on some kind of computing device. It is artificial to claim that software must be viewed in isolation from the computing device on which it runs and with which it is inseparable in regard to the challenged conduct.” *James v. Walt Disney Co.*, 701 F. Supp. 3d 942, 958 (N.D. Cal. 2023).

171. Defendant procured the interception of communications between Plaintiff McGuire and Pennsylvania Subclass members and the Criterion Channel Service that were subsequently redirected to and recorded by the Third Parties without Plaintiff McGuire or Pennsylvania Subclass members’ consent.

172. Plaintiff McGuire and Pennsylvania Subclass members had a justified expectation

under the circumstances that their electronic communications would not be intercepted by the Third Parties. Not only did Plaintiff McGuire and Pennsylvania Subclass members have a reasonable expectation of privacy in their PII (such as full names, e-mail addresses, and Meta IDs), Congress has declared that consumers have a right to the privacy of their video-viewing information, as such information is “a window into our loves, likes, and dislikes.” S. Rep. No. 100-599 at 6-7 (1988) (remarks by Senator Paul Simon).

173. The wiretapping of Plaintiff McGuire and Pennsylvania Subclass members occurred in Pennsylvania, where Plaintiff McGuire and Pennsylvania Subclass Members accessed the Criterion Channel Service and where the Third Parties—as procured by Defendant—routed Plaintiff McGuire’s and Pennsylvania Subclass members’ electronic communications to the Third Parties’ respective servers. *Popa*, 52 F.4th at 131.

174. WESCA confers a private cause of action on any person whose wire, electronic, or oral communication is intercepted, disclosed, or used in violation thereof against “any person who intercepts, discloses, or uses or procures any other person to intercept, disclose or use, such communication.” 18 Pa. Cons. Stat. § 5725(a).

175. Plaintiff McGuire seeks, on behalf of himself and each Pennsylvania Subclass member, (i) actual damages, not less than liquidated damages computed at the rate of \$100/day or \$1,000 for each violation, whichever is higher; (ii) punitive damages; and (iii) reasonable attorneys’ fees and other litigation costs incurred. 18 Pa. Cons. Stat. § 5725(a).

COUNT IV
Violation Of The Florida Security Of Communications Act,
Fla. Stat. §§ 934.01, *et seq.*

176. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

177. Plaintiff Wickham brings this claim individually and on behalf of the proposed

Florida Subclass against Defendant.

178. The FSCA makes it illegal for a person to “intentionally intercept[], endeavor[] to intercept, or procure[] any other person to intercept or endeavor to intercept any wire, oral or electronic communication.” Fla Stat. § 934.03(1)(a).” Further, the FSCA prohibits the “use,” “disclosure,” or any endeavors to use or disclose the contents of such intercepted communications. Fla. Stat. § 934.03(1)(b)-(e).

179. The FSCA further permits a private civil claim:

Any person whose wire, oral, or electronic communication is intercepted, disclosed, or used in violation of ss. 934.03-934.09 shall have a civil cause of action against any person or entity who intercepts, discloses, or uses, or procures any other person or entity to intercept, disclose, or use, such communications and shall be entitled to recover from any such person or entity which engaged in that violation such relief as may be appropriate, including: ... (b) Actual damages, but not less than liquidated damages, computed at the rate of \$100 a day for each day of violation or \$1,000, whichever is higher; (c) Punitive damages; and (d) A reasonable attorney’s fee and other litigation costs reasonably incurred.

Fla. Stat. § 934.10(1).

180. Defendant and the Third Parties are each a “person or entity” for purposes of the FSCA because they are corporations.

181. The Third Parties’ software that Defendant implemented into the Criterion Channel Service each constitute a “device” that is “affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication” within the meaning of the Fla. Stat. § 934.03.

182. Plaintiff Wickham’s and Florida Subclass members’ intercepted information and communications constitute a “wire, oral or electronic communication” within the meaning of the statute. *Id.*

183. Plaintiff Wickham’s and Florida Subclass members’ electronic communications

were intercepted contemporaneously with their transmission. Defendant then “disclose[s]” and “use[s]” such intercepted communications for its own benefit.

184. Plaintiff Wickham and Florida Subclass members did not consent to having their activity and communications with the Criterion Channel Service wiretapped.

185. Pursuant to Fla. Stat. § 934.10, Plaintiff Wickham and Florida Subclass members seek (i) actual damages, not less than liquidated damages computed at the rate of \$100 a day for each day of violation or \$1,000 dollars, whichever is higher, (ii) punitive damages, and (iii) reasonable attorneys’ fees and other costs of litigation incurred.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs seek a judgment against Defendant, individually and on behalf of all others similarly situated, as follows:

- (a) For an order certifying the Classes under Rule 23 of the Federal Rules of Civil Procedure, naming Plaintiffs as representative of the Classes, and naming Plaintiffs’ attorneys as Class Counsel to represent the Classes;
- (b) For an order declaring that Defendant’s conduct violates the statutes referenced herein;
- (c) For an order finding in favor of Plaintiffs and the Classes on all counts asserted herein;
- (d) An award of statutory damages to the extent available;
- (e) For punitive damages, as warranted, in an amount to be determined at trial;
- (f) For prejudgment interest on all amounts awarded;
- (g) For an order awarding Plaintiffs and the Classes their reasonable attorneys’ fees and expenses and costs of suit.

JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b)(1), Plaintiffs demand a trial by jury of all issues so triable.

Dated: December 6, 2024

Respectfully submitted,

BURSOR & FISHER, P.A.

By: /s/ Yitzchak Kopel
Yitzchak Kopel

Yitzchak Kopel
Max S. Roberts
Victoria X. Zhou
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-Mail: ykopel@bursor.com
mroberts@bursor.com
vzhou@bursor.com

LEVI & KORSINSKY, LLP

Mark S. Reich
Gary S. Ishimoto*
33 Whitehall Street, Floor 17
New York, NY 10004
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: mreich@zlk.com
Email: gishimoto@zlk.com

**Pro Hac Vice Forthcoming*

Attorneys for Plaintiffs