

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

MAXWELL HARWELL individually and on  
behalf of all others similarly situated,

Plaintiff,

v.

MCGRAW HILL LLC,

Defendant.

Civil Action No.:

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

Dated: September 24, 2024

**BURSOR & FISHER, P.A.**

Yitzchak Z. 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

Email: ykopel@bursor.com

mroberts@bursor.com

vzhou@bursor.com

*Attorneys for Plaintiff*

**TABLE OF CONTENTS**

NATURE OF THE ACTION ..... 1

PARTIES ..... 2

JURISDICTION AND VENUE ..... 2

FACTUAL ALLEGATIONS ..... 3

I. Overview and History of the VPPA..... 3

II. Defendant Is A Video Tape Service Provider..... 4

III. Defendant Knowingly Discloses Consumers’ Personally Identifiable Information To Third Parties..... 6

    A. Testing Reveals Defendant Illegally Shares Consumers’ PII With Third Parties Through Its Sharpen App..... 7

    B. Defendant Illegally Shares Consumers’ PII With Third Parties Through The Sharpen Website ..... 11

    C. Defendant Discloses Personally Identifiable Information To The Third Parties For The Purposes Of Marketing, Advertising, And Analytics ..... 24

    D. Defendant Knowingly Discloses Its Users’ PII To The Third Parties..... 28

IV. Plaintiff’s Experience..... 29

CLASS ALLEGATIONS ..... 31

JURY TRIAL DEMANDED ..... 35

Plaintiff Maxell Harwell (“Plaintiff”) brings this action on behalf of himself and all others similarly situated against Defendant McGraw Hill, LLC, d/b/a Sharpen (“Defendant”).

### **NATURE OF THE ACTION**

1. This is a class action suit brought against Defendant for violating the Video Privacy Protection Act (“VPPA”).

2. The United States Congress passed the VPPA in 1988, seeking to confer onto consumers the power to “maintain control over personal information divulged and generated in exchange for receiving services from video tape service providers.” S. Rep. No. 100-599, at 8. “The Act reflects the central principle of the Privacy Act of 1974: that information collected for one purpose may not be used for a different purpose without the individual’s consent.” *Id.*

3. 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.

4. Defendant owns and operates Sharpen, a “College Study App” that “makes studying simple, fun, and achievable with short videos and study tools that get straight to the point.”<sup>1</sup> Defendant’s videos are pre-recorded videos.

5. The Sharpen mobile application is accessible through both the Android and iOS app stores (the “App”), and is also readily available in a web browser format at “mheducation.com/sharpen/study-app.html” (the “Website”).

---

<sup>1</sup> See, e.g., Sharpen, GOOGLE STORE, <https://play.google.com/store/apps/details?id=com.mheducation.redi>; Sharpen, IOS APP STORE, <https://apps.apple.com/us/app/sharpen-college-exam-prep/id1595642363>.

## Meet your new **study app**: your textbook, simplified.

Don't just use your textbook. Learn the same content faster with short videos, mini quizzes, and flashcards.

**Find your study tools by textbook or topic:**

See All Titles on Sharpen

6. Unbeknownst to Plaintiff and the Class Members, Defendant knowingly and intentionally discloses their users' personally identifying information, along with a record of every video viewed by the user, to unrelated third parties. By doing so, Defendant violated the VPPA.

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

### **PARTIES**

8. Plaintiff Maxwell Harwell is a resident of New Jersey.

9. Defendant McGraw Hill LLC is a Delaware limited liability company whose principal place of business is 1325 Avenue of the Americas, New York, New York 10019.

Defendant McGraw Hill LLC owns and operates the Apps and the Website.

### **JURISDICTION AND VENUE**

10. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because this case arises under a law of the United States (*i.e.*, the VPPA).

11. This Court has personal jurisdiction over Defendant because is domiciled in this District.

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

## **FACTUAL ALLEGATIONS**

### **I. OVERVIEW AND HISTORY OF THE VPPA**

13. The impetus for the VPPA began 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 Pratik 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 (internal ellipses and brackets omitted).

14. In 2012, Congress amended the VPPA, and in so doing, reiterated the Act’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.

15. 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).

## **II. DEFENDANT IS A VIDEO TAPE SERVICE PROVIDER**

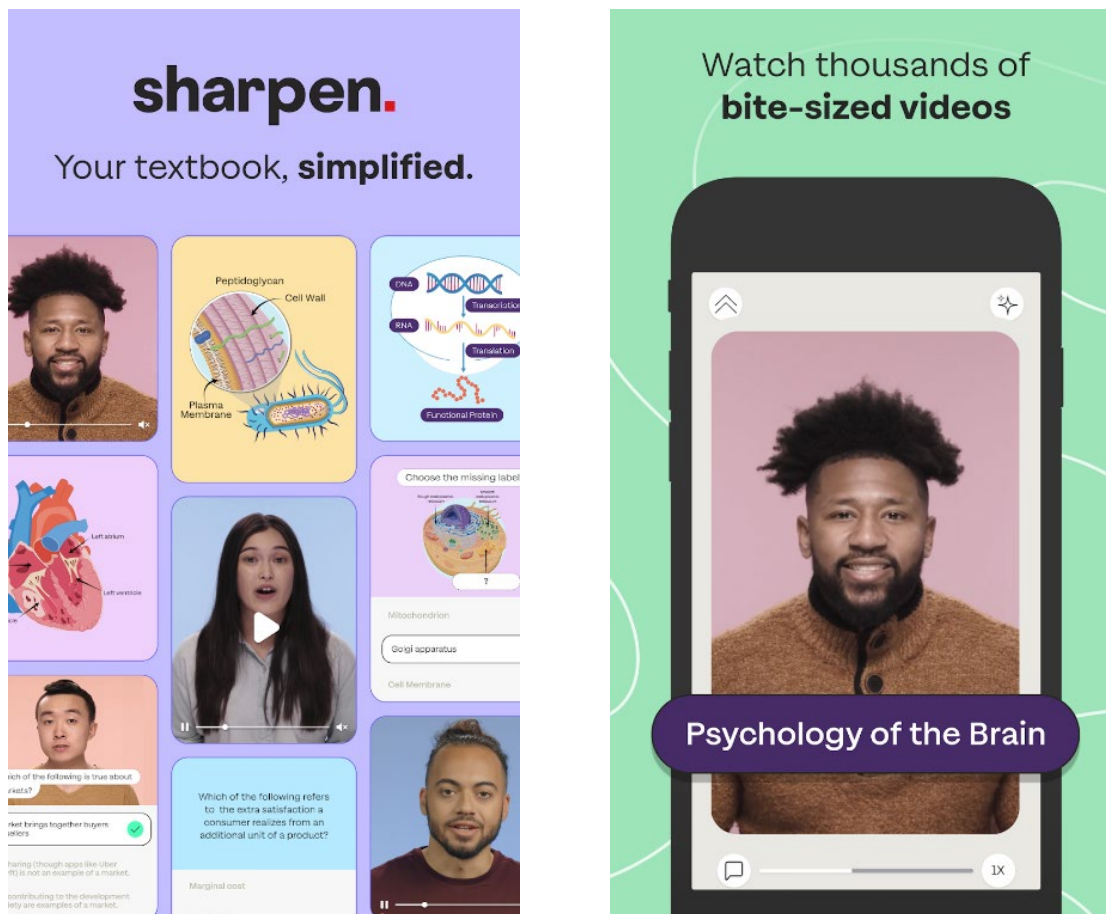
16. The App is available for download and use throughout the United States, including in New Hampshire.

17. Defendant’s App hosts and delivers, upon request, “thousands of bite-sized videos.” The videos are all prerecorded educational programs and lectures covering a wide variety of subjects. The consumer, when using the App, is presented with a host of subject tabs, underneath which contain lectures and explanatory videos.

18. The offering of these videos is critical to Defendant’s product and business as a study-aid service. In fact, Defendant even promotes its Sharpen service as a simplified textbook for the consumer to “know what to focus on with short videos that teach the key concepts in each subject.”<sup>2</sup>

---

<sup>2</sup> Sharpen, GOOGLE PLAY STORE, [https://play.google.com/store/apps/details?id=com.mheducation.redi&hl=en\\_US](https://play.google.com/store/apps/details?id=com.mheducation.redi&hl=en_US).



19. Only users with accounts may access Defendant’s content, including all of Defendant’s pre-recorded video content.<sup>3</sup> To sign up for and create an account, users must provide their PII, including name and email address, to Defendant.

20. The App is available for Android, iOS, and Sharpen is also accessible on web browsers. Both the App and Website versions of Sharpen provide access to the same pre-recorded videos and materials, and all formats of Sharpen disclose, as shown below, the users’

<sup>3</sup> See, e.g., Create a Sharpen Account, SHARPEN, <https://app.studysharpen.com/sign-up?courseId=01H7CJ00C7B3KQ52CH25DPCEAY&sectionId=01H7CJ010H6PKB3M879F7VZBWB&stackId=01H7CJ0280D291Y8PHY1WFSNQY> (users must first enter their email addresses and full names to continue to watch any pre-recorded video). While users can initially view a video without signing up, the Website and App force them to register accounts prior to watching subsequent videos.

personally identifiable information along with the videos watched in substantially the same manner to third parties.

### **III. DEFENDANT KNOWINGLY DISCLOSES CONSUMERS' PERSONALLY IDENTIFIABLE INFORMATION TO THIRD PARTIES**

21. In the summer of 2024, Plaintiff's counsel retained a private research company to review the App and conduct a dynamic analysis. A "dynamic analysis" records the transmissions that occur from a user's device.

22. The researchers tested what information (if any) was disclosed when a user watches a video on the App. The analysis revealed that Defendant discloses information to third parties sufficient to identify specific Class Members and the specific videos they watched.

23. The analysis first established that Defendant incorporates multiple "application programming interfaces" ("APIs") into its App.

24. APIs "enable[] companies to open up their applications' data and functionality to external third-party developers, business partners, and internal departments within their companies."<sup>4</sup>

25. An API can "work[] as a standalone solution or included within an SDK. ... [A]n SDK often contains at least one API."<sup>5</sup> "SDK stands for software development kit and "ios a set of software-building tools for a specific program, while "API" stands for application programming interface.<sup>6</sup> As used in this Complaint, "SDK" and "API" are referring to the same software.

---

<sup>4</sup> Michael Goodwin, *What is an API? (Application Programming Interface)*, IBM, <https://www.ibm.com/cloud/learn/api>.

<sup>5</sup> SDK VS. API: WHAT'S THE DIFFERENCE?, IBM (July 13, 2011), <https://www.ibm.com/blog/sdk-vs-api/>.

<sup>6</sup> *Id.*



26. Defendant integrates multiple companies' SDKs and similar packets of tracking code into the App and Website, including but not limited to the: Segment SDK, Sprig SDK, Braze SDK, and the Meta Tracking Pixel.

**A. Testing Reveals Defendant Illegally Shares Consumers' PII With Third Parties Through Its Sharpen App**

27. Defendant incorporates into the iOS and Android App at least one SDK: the Segment SDK, an API owned and operated by Twilio.

28. The dynamic analysis found that when a user views a video on the App on either an Android or iOS mobile device, Defendant transmits information sufficient to permit an ordinary person to identify a specific person's video-viewing behavior to Twilio.

29. Specifically, when a user views a video in the App, Defendant discloses to Twilio via the Segment SDK the users' (i) name, (ii) email address, (iii) User ID, (iv) the title of the specific video viewed, (v) the video ID, and (vi) the fact that the specific video was actually watched or viewed by the user.

*i. Overview of the Segment SDK*

30. Twilio is a software company that allows developers like Defendant to “[h]arness [their] customer data to power omnichannel, personalized engagement.”<sup>7</sup>

31. Twilio powers this platform through its Segment API, which offers “world-class customer data infrastructure, so [developers] can design hyper-personalized, omnichannel campaigns across all channels.”<sup>8</sup> In particular, once integrated into a developer's mobile application, the Segment API provides Twilio's platform with “customer identification and

---

<sup>7</sup> Twilio, <https://www.twilio.com/en-us/customer-engagement-platform>.

<sup>8</sup> Twilio + Segment, SEGMENT, <https://segment.com/twilio/>.

segmentation[,]”<sup>9</sup> doing so 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.”<sup>10</sup>

32. As alleged in greater detail below, Defendant utilizes each and every one of these features of the Segment SDK in the App and sends its consumers’ PII to Twilio through the Segment SDK in order to assist with Defendant’s marketing, advertising, and analytics efforts.

ii. *Testing Reveals Defendant Discloses iOS App Users’ Full Names and Email Addresses To Segment*

33. A user’s full name is self-evidently personally identifiable information, as it is the means of identifying individuals in all aspects of their lives.

34. An email address is a unique string of characters which designate an electronic mailbox. As industry leaders,<sup>11</sup> trade groups,<sup>12</sup> and courts agree,<sup>13</sup> an ordinary person can use an email address to uniquely identify another individual.

35. Indeed, there exists multiple services that enable anyone with internet access and a credit card to look up who owns a particular email address.<sup>14</sup>

---

<sup>9</sup> 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/>.

<sup>10</sup> MParticle Analytic, INDICATIVE, <https://www.indicative.com/resource/segment-io/>.

<sup>11</sup> 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”).

<sup>12</sup> Network Advertising Initiative, NAI CODE OF CONDUCT 19 (2019), [https://thenai.org/wp-content/uploads/2021/07/nai\\_code2020.pdf](https://thenai.org/wp-content/uploads/2021/07/nai_code2020.pdf) (identifying email as PII).

<sup>13</sup> *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.”).

<sup>14</sup> *See, e.g., BEENVERIFIED*, [www.beenverified.com](http://www.beenverified.com).

36. The following excerpt from the dynamic analysis demonstrates Defendant transmitting an iOS user's full name and email address to Twilio via the Segment SDK:

```
"full_name": "Johnny Smith",  
"email": "johnnysmithemail7@gmail.com",
```

37. In addition, Defendant also discloses to Twilio through the Segment SDK a user's "anonymousID"—another form of unique identification for each individual user that Twilio assigns. Twilio uses the "anonymousID" in addition to the other personally identifying information and video viewing information that Defendant transmits to Twilio in its marketing, advertising, and analytics processes for Defendant.

```
"anonymousId": "DF103DAD-E72B-4DEF-A217-B0EB1A87DD01"
```

*iii. Testing Reveals Defendant Discloses Android App Users' Email Addresses, First Names, and User IDs To Segment*

38. As discussed above, an email address is a unique string of characters that can be used to uniquely identify an individual linked to the specific electronic mailbox associated with the email address.

39. Defendant discloses to Twilio through the Segment APIs and SDK Sharpen Android App users' first names and email addresses, as shown in the following screenshot of the excerpted dynamic analysis:

```
courses_completed : 0,  
"email": "beegoodkay@gmail.com",  
"email_notifications_on": "false",  
"full_name": "Benjamin",  
"id":
```

40. The fact that a user's first name is disclosed in addition to their email address only further distinguishes each unique email address and identifies it as the electronic mailbox

associated with an individual user. This, in turn, allows Segment to provide Defendant with more detailed categorization capacity to enhance its marketing, analytics, and advertisement capabilities.

41. Simultaneously, Defendant also transmits to Segment a user's unique User ID. This is a unique string of letters, numbers, and hyphens that identifies a given user for Segment and Defendant. Segment uses the User ID to provide Defendant with further capabilities to market, analyze its user base, and advertise to its users.

```
"urn:com.mheducation.openlearning:enterprise.identity:prod.us-east-1:person:1984670a-42b1-4736-8686-81e7c890a29d"
```

*iv. Defendant Discloses Information Identifying Which Specific Videos Were Watched By Which Specific App Users To Segment*

42. Defendant discloses to Twilio, through the Segment SDK, the video title, video ID, and interactions of users who watch videos on the Sharpen iOS App. The following screenshot depicts Defendant transmitting to Twilio an iOS user's video-viewing information, including the full title of the watched video: "Sequences, Series, Induction, and Probability." Defendant calls this both the "activity\_name" and the "concept\_name" in its transmissions to Segment.

```
"activity_name": "Sequences, Series, Induction, and Probability",
"concept_id": "01H7CR2MECH9AWE79DRY2F9DKM",
"ui_presentation_order": 1,
"concept_name": "Sequences, Series, Induction, and Probability",
```

43. Defendant discloses to Twilio, through the Segment SDK, the video title, video ID (shown as the "content\_id" field below), and the interactions of users who watch videos on the Sharpen Android App. The following screenshot depicts Defendant transmitting to Twilio an Android user's video-viewing information, including the full title of the watched video: "Contemporary Approaches to Psychology."

```
"activity_content_type": "video",
"activity_id": "01H7CHMN10S5JA43XJRNCHM53",
"activity_length": "1",
"activity_name": "Contemporary Approaches to Psychology",
"activity_type": "overview",
"concept_id": "01H7CHKBJ7Y1NJGKMB5C1KBFHX",
"concept_name": "The Science of Psychology ",
"content_id": "01H7CHMFV4B1H10PZQRWF8ZCQY"
```

44. Notably, Defendant discloses to Twilio information sufficient to prove that a given Android user actually watched a Sharpen video by also disclosing that the video was played in the simultaneously disclosed “event” field:

```
"event": "Video Started",
"interactions": {
```

**B. Defendant Illegally Shares Consumers’ PII With Third Parties Through The Sharpen Website**

45. Defendant also incorporates onto its Website multiple SDKs and similar packets of tracking code.<sup>15</sup> These SDKs and packets of code act as the SDKs for the Sharpen mobile applications do to capture and transmit Website users’ personally identifiable information to third parties. Defendant integrates at least three onto its Website: the Sprig SDK, the Meta Tracking Pixel, and the Braze SDK.

46. The following table depicts the categories of PII being shared with third parties:

<i>THIRD PARTY</i>	<i>VIDEO INFO</i>	<i>PERSONAL INFO</i>	<i>OTHER INFO</i>
<b>Meta</b>	Video Title, Video ID, Video Interactions	Email (hashed), First Name	User ID, FBP
<b>Sprig</b>	Video Title, Video ID, Video Interactions	Email (plain), First Name	User ID
<b>Braze</b>	Video Title, Video ID, Video Interactions	Email (plain), First Name	User ID

<sup>15</sup> Similar to how SDKs can be integrated into a mobile application to track users’ personally identifiable information, SDKs can also be integrated onto a website.

*i. Overview Of The Sprig SDK*

47. Sprig is a “product experience platform that empowers teams to fuel product growth with AI insights.”<sup>16</sup> Sprig boasts it can assist customers like Defendant to “properly analyze” “[u]ser behavior data,” so as to “help [Defendant] detect pain points, evaluate user behavior, test new features, and improve [its] product. Understanding that data in context is key to unlocking those game-changing insights.”<sup>17</sup>

48. Sprig offers several user-tracking functions including “Replays,” “Heatmaps,” “Surveys,” “Feedback,” and “AI Analysis.”<sup>18</sup> “Replays captures trigger-based user journey clips” including “watch[ing] users as they engage with features for the first time and identify areas for optimization.”<sup>19</sup> Heatmaps allows the site to “capture a visual representation of [the] users’ in-product interacts” to “[u]nderstand user engagement trends across [the] product experience in real time to help [] boost adoption, retention, and satisfaction.”<sup>20</sup> “Surveys” offers in-product targeted surveys to users.<sup>21</sup> Similarly, “Feedback” allows the site to “collect continuous feedback right in [the] product.”<sup>22</sup> Sprig’s technological toolset also includes a data collection tool that Sprig calls “User Interviews.”<sup>23</sup> This tool allows Defendant to “collect real-time insights from the right users.”<sup>24</sup>

---

<sup>16</sup> About Sprig, SPRIG, <https://docs.sprig.com/docs/what-is-sprig>.

<sup>17</sup> How to Analyze Data from Session Replays, SPRIG (July 26, 2024), <https://sprig.com/blog/how-to-analyze-data-from-session-replays>.

<sup>18</sup> What is Sprig, SPRIG, <https://docs.sprig.com/docs/what-is-sprig>.

<sup>19</sup> *Id.*

<sup>20</sup> *Id.*

<sup>21</sup> *Id.*

<sup>22</sup> *Id.*

<sup>23</sup> User Interviews, SPRIG, <https://docs.sprig.com/docs/user-interviews>.

<sup>24</sup> *Id.*

49. A main Sprig feature is the Sprig “Study.”<sup>25</sup> Three types of so-called Studies exist, each with its own analytical benefits: “surveys,” which are “a set of questions that can be delivered to respondents;” “Replays,” which capture “session clips of ... users’ experience captured alongside their in-product feedback;” and “feedback,” which allows Defendant to “capture continuous user-initiated feedback via an easily customizable button.”<sup>26</sup>

50. Sprig Studies work to allow companies like Defendant “to monitor [their] customer’s interactions and generate triggers to launch a Sprig Survey or Replay, so you can ask just the right question and capture just the right moments—all at just the right time.”<sup>27</sup> Specifically, events, including “visiting a page, clicking a button, and scrolling to a specific position on a page,” “are used to trigger” Studies.<sup>28</sup>

51. “[T]o help [Defendant] organize [its] studies” and compile analyzed user data in a read-friendly format, Sprig also offers solutions such as “Dashboards” and “Folders.”<sup>29</sup> “Dashboards” allow Defendant to “monitor and track the study results,” offering spreadsheet-like capabilities to “group ... studies by product owner, subject, timeframe, product line, or team.”<sup>30</sup> “Folders” allow Defendant “to organize studies into categories.”<sup>31</sup>

---

<sup>25</sup> Study Creation, SPRIG, <https://docs.sprig.com/docs/main-tasks>.

<sup>26</sup> *Id.*

<sup>27</sup> Web, SPRIG, <https://docs.sprig.com/docs/introduction-web>.

<sup>28</sup> Web & Mobile Studies, SPRIG, <https://docs.sprig.com/docs/web-mobile>. “An event can be any action in your web or mobile application that allows you to track user behavior.” *Id.*

<sup>29</sup> Dashboard and Folders, SPRIG, <https://docs.sprig.com/docs/dashboards-and-folders>.

<sup>30</sup> *Id.*

<sup>31</sup> *Id.*

The screenshot shows the Sprig website header with navigation links: Products, Solutions, Templates, and Customers. Below the header, the 'BY USE CASE' section lists four categories:

- Continuously optimize**: Analyze your users' experience through core flows.
- Improve conversion**: Understand why and how users are dropping off.
- Solve pain points**: Uncover emerging trends in your users' behavior.
- Save time & resources**: Know which new features are worth the investment.

ii. *Overview Of The Meta Tracking Pixel*

52. Meta (formerly known as Facebook) describes itself as a “real identity platform,”<sup>32</sup> and is the largest social networking site on the planet, touting 2.9 billion monthly active users.<sup>33</sup> Meta users are allowed only one account and must share “the name they go by in everyday life.”<sup>34</sup> To that end, when creating an account, users must provide their first and last name, along with their birthday and gender.<sup>35</sup>

<sup>32</sup> Sam Schechner and Jeff Horwitz, *How Many Users Does Facebook Have? The Company Struggles to Figure It Out*, WALL. ST. J. (Oct. 21, 2021), <https://www.wsj.com/articles/how-many-users-does-facebook-have-the-company-struggles-to-figure-it-out-11634846701>.

<sup>33</sup> Sean Burch, *Facebook Climbs to 2.9 Billion Users, Report 29.1 Billion in Q2 Sales*, YAHOO (July 28, 2021), <https://www.yahoo.com/now/facebook-climbs-2-9-billion-202044267.html>.

<sup>34</sup> Community Standards, Part IV Integrity and Authenticity, META, [https://www.facebook.com/communitystandards/integrity\\_authenticity](https://www.facebook.com/communitystandards/integrity_authenticity).

<sup>35</sup> Sign Up, META, <https://www.facebook.com/>.



53. Meta generates revenue by selling advertising space on its website.<sup>36</sup> In 2022, Meta generated over \$116 billion in revenue.<sup>37</sup> Roughly \$113.6 billion of that, or 97.9%, came from selling advertising space.<sup>38</sup>

54. Meta sells advertising space by highlighting its ability to target users.<sup>39</sup> Meta can target users so effectively because it surveils user activity both on and off its site.<sup>40</sup> This allows Meta to make inferences about users beyond what they explicitly disclose, like their “interests,” “behavior,” and “connections.”<sup>41</sup> Meta compiles this information into a generalized dataset called “Core Audiences,” which advertisers use to apply highly specific filters and parameters for their targeted advertisements.<sup>42</sup>

55. Advertisers, such as Defendant, can also build “Custom Audiences.”<sup>43</sup> Custom Audiences enable advertisers to reach “people who have already shown interest in [their] business, whether they’re loyal customers or people who have used [their] app or visited [their] website.” With Custom Audiences, advertisers can target existing customers directly, and can also build

---

<sup>36</sup> Mike Isaac, *Facebook’s profit surges 101 percent on strong ad sales.*, N.Y. TIMES (July 28, 2021), <https://www.nytimes.com/2021/07/28/business/facebook-q2-earnings.html>.

<sup>37</sup> Meta Reports Fourth Quarter and Full Year 2022 Results, META, <https://investor.fb.com/investor-news/press-release-details/2023/Meta-Reports-Fourth-Quarter-and-Full-Year-2022-Results/default.aspx>.

<sup>38</sup> Derek Lewis, *Meta and Alphabet Earnings: Ad Revenue in Focus*, YAHOO FINANCE (Oct. 20, 2023), <https://finance.yahoo.com/news/meta-alphabet-earnings-ad-revenue-231700102.html?guccounter=2>.

<sup>39</sup> Why Advertise on Meta, META, <https://www.facebook.com/business/help/205029060038706>.

<sup>40</sup> About Meta Pixel, META, <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>.

<sup>41</sup> Ad Targeting: Help Your Ads Find The People Who Will Love Your Business, META, <https://www.facebook.com/business/ads/ad-targeting>.

<sup>42</sup> Easier, More Effective Ways to Reach the Right People on Facebook, META, <https://www.facebook.com/business/news/Core-Audiences>.

<sup>43</sup> About Custom Audiences, META, <https://www.facebook.com/business/help/744354708981227?id=2469097953376494>.

“Lookalike Audiences,” which “leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities.”<sup>44</sup>

56. Unlike Core Audiences, Custom Audiences require an advertiser to supply the underlying data to Meta. Advertisers can do this through two mechanisms: (i) by manually uploading contact information for customers, or (ii) by utilizing Meta’s “Business Tools,” which collect and transmit the data automatically.<sup>45</sup> One such Business Tool is the Meta Tracking Pixel.

57. The Meta Tracking Pixel is a piece of code that advertisers, like Defendant, can integrate into their website. Once activated, the Meta Tracking Pixel “tracks the people and type of actions they take.”<sup>46</sup>

58. When the Meta Tracking Pixel captures an action, it sends a record to Meta. Once this record is received, Meta processes it, analyzes it, and assimilates it into datasets like Custom Audiences and Core Audiences.

59. Defendant can control what actions—or, as Meta calls it, “events”—the Meta Tracking Pixel will collect. The Meta Tracking Pixel can capture the website’s metadata, along with what pages a visitor views and what buttons a visitor clicks.<sup>47</sup> Defendant can also configure the Meta Tracking Pixel to track other events. Meta offers a menu of “standard events” from which

---

<sup>44</sup> About Lookalike Audiences, META, <https://www.facebook.com/business/help/164749007013531?id=401668390442328>.

<sup>45</sup> Create a Customer List Custom Audience, META, <https://www.facebook.com/business/help/170456843145568?id=2469097953376494>.

<sup>46</sup> Retargeting, META, <https://www.facebook.com/business/goals/retargeting>.

<sup>47</sup> See Meta Pixel, Accurate Event Tracking, META, <https://developers.facebook.com/docs/facebook-pixel/advanced/>; see also Best Practices for Meta Pixel Setup, META, <https://www.facebook.com/business/help/218844828315224?id=1205376682832142>.

advertisers like Defendant can choose, including what content a visitor views or purchases.<sup>48</sup> Defendant can also create its own tracking parameters by building a “custom event.”<sup>49</sup>

60. Website developers like Defendant control how the Meta Tracking Pixel identifies Website visitors. The Meta Tracking Pixel is configured to automatically collect “HTTP Headers” and “Pixel-specific Data.”<sup>50</sup> HTTP Headers collect “IP addresses, information about the web browser, page location, document, referrer and persons using the website.”<sup>51</sup> Pixel-specific Data includes “the Pixel ID and cookie.”<sup>52</sup>

*iii. Overview Of The Braze SDK*

61. Braze is another third-party SDK that provides a “customer engagement platform” that “power[s] customer-centric interactions between the consumers and brands in real-time.”<sup>53</sup> Defendant utilized Braze to assist with its marketing, advertising, and analytics efforts.

62. Once integrated into a developer’s website, the Braze SDK allows developers such as Defendant to, among other features, “conduct analytics” by “set[ting] user IDs for each” user, then using those user IDs in conjunction with other disclosed PII to “[t]rack[] custom events”

---

<sup>48</sup> Specifications for Facebook Pixel Standard Events, META, <https://www.facebook.com/business/help/402791146561655?id=1205376682832142>.

<sup>49</sup> Meta Pixel, META, <https://developers.facebook.com/docs/meta-pixel/>.

<sup>50</sup> *Id.*

<sup>51</sup> *Id.*

<sup>52</sup> *Id.*

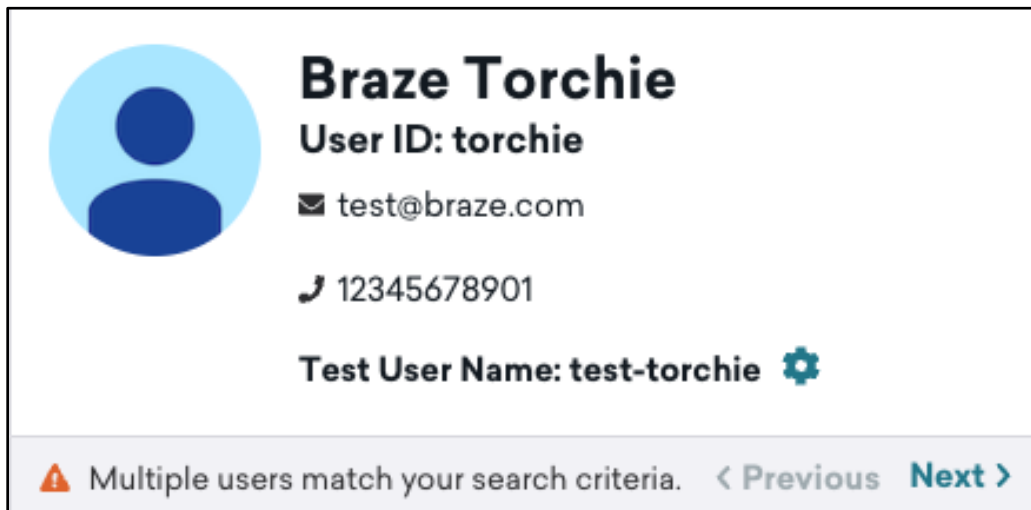
<sup>53</sup> Launch Your Marketing With the Platform Purpose-Built for Customer Engagement, BRAZE, [https://www.braze.com/brand?utm\\_medium=paid-search&utm\\_source=google&utm\\_campaign=fy22-amer-brand\\_1\\_brand&utm\\_content=&utm\\_term=braze\\_crm|braze%20crm|p|g|c|691187167367&\\_bt=691187167367&\\_bk=braze%20crm&\\_bm=p&\\_bn=g&gad\\_source=1&gclid=CjwKCAjwqre1BhAqEiwA7g9QhnUvoOBPdPyAEqD1zuK\\_vhpYC6v9y-LnVaotAxbLzX50LrAps9ltgRoC0uMQAvD\\_BwE](https://www.braze.com/brand?utm_medium=paid-search&utm_source=google&utm_campaign=fy22-amer-brand_1_brand&utm_content=&utm_term=braze_crm|braze%20crm|p|g|c|691187167367&_bt=691187167367&_bk=braze%20crm&_bm=p&_bn=g&gad_source=1&gclid=CjwKCAjwqre1BhAqEiwA7g9QhnUvoOBPdPyAEqD1zuK_vhpYC6v9y-LnVaotAxbLzX50LrAps9ltgRoC0uMQAvD_BwE).

“across devices and platforms, improving the quality of [Defendant’s] behavioral and demographic data,” “[i]mport data about [Defendant’s] users,” and “[t]arget specific users.”<sup>54</sup>

63. Braze helps developers like Defendant market, advertise, and analyze real-time user data in order to build precise audiences that can “[i]dentify, target and engage customers based on their likelihood to purchase or perform any other high value action.”<sup>55</sup>

64. The data Braze collects is not just from one source. On the contrary, developers can integrate customer data from a variety of sources into Braze. Using this data, developers can then utilize Braze’s analytics to obtain a “unified view” of their customers in order to “act on real-time and historical preferences [and] behaviors” to target them more effectively.

65. Braze conglomerates all of this data into user profiles, which it associates with identifiers like a Braze user ID and/or e-mail address.<sup>56</sup>



<sup>54</sup> Setting user IDs, BRAZE, [https://www.braze.com/docs/developer\\_guide/platform\\_integration\\_guides/web/analytics/setting\\_user\\_ids](https://www.braze.com/docs/developer_guide/platform_integration_guides/web/analytics/setting_user_ids); Tracking custom events, BRAZE, [https://www.braze.com/docs/developer\\_guide/platform\\_integration\\_guides/web/analytics/tracking\\_custom\\_events](https://www.braze.com/docs/developer_guide/platform_integration_guides/web/analytics/tracking_custom_events).

<sup>55</sup> Data & Analytics, BRAZE, <https://www.braze.com/product/data-and-analytics>.

<sup>56</sup> User Profiles, BRAZE, [https://www.braze.com/docs/user\\_guide/engagement\\_tools/segments/user\\_profiles/#access-profiles](https://www.braze.com/docs/user_guide/engagement_tools/segments/user_profiles/#access-profiles).

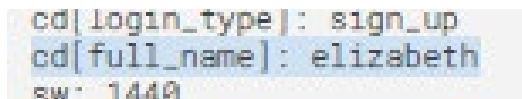
66. As Braze collects more data however, the user profiles become even more detailed. These detailed user profiles could include data related to a user's location, gender, age group, operating system, actions taken on a website, and even if a user has a credit card or not.<sup>57</sup>

67. Notably, Braze does not collect all of this data by default. Instead, its default settings only allow Braze to collect data such as time zone and browser types.<sup>58</sup> Rather, developers like Defendant must *specifically enable or configure* the Braze SDK to collect additional data such as e-mail addresses and geolocation.<sup>59</sup>

68. Defendant uses each and every one of the above-mentioned features of the Braze SDK in Defendant's integration of the Braze SDK into Defendant's Website. Thus, Defendant utilizes the Braze SDK to analyze user data, create and analyze the performance of marketing campaigns, and target specific users or specific groups of users for advertisements. All of this helps Defendant further monetize the Website and maximize revenue by collecting and disclosing as much PII as possible to Braze through the Braze SDK.

iv. *Defendant Discloses Users' Email Addresses, First Names, And User IDs To Meta, Sprig, And Braze*

69. **Meta.** Defendant discloses to Meta through the Meta Tracking Pixel a user's email address, first name, Meta FBP cookie, and User ID. The following screenshots depict Defendant doing so:



```
cd[login_type]: sign_up
cd[full_name]: elizabeth
sw: 1440
```

<sup>57</sup> *See id.*

<sup>58</sup> SDK Data Collection, BRAZE, [https://www.braze.com/docs/user\\_guide/data\\_and\\_analytics/user\\_data\\_collection/sdk\\_data\\_collection/?redirected=true#personalized-integration](https://www.braze.com/docs/user_guide/data_and_analytics/user_data_collection/sdk_data_collection/?redirected=true#personalized-integration).

<sup>59</sup> *Id.* (noting that default information collected does not include users' geolocation, emails, or names, and "[t]o make the most out of Braze, our SDK integrators often implement the Braze SDKs and log custom attributes, custom events and purchase events that are pertinent to their business on top of the automatically collected data.").

```
sh: 900
ud[external_id]: 3794d9f5c07f856ded1c0d192e0483e45066fab3008384ba66d01e90912edefa
udff[em]: 4fd99119458274f6087074b65cbee546b089f9d8581f1b0a291f96884dc18da5
udff[fn]: b54f08623ae4039f55bcecba4961037fb4513d2ba9cb2b0667c5db970ac94911
v: 2.9.161
```

```
fbp: fb.1.1721062497866.242157908188424757
Label: other
```

70. The field labeled “udff[em]” represents the user’s email address, and the field labeled “udff[fn]” represents the user’s disclosed first name.<sup>60</sup> The string of numbers and letters after the colon for both represents the encrypted email address and first name. This was done using an encryption format called “SHA 256.”<sup>61</sup> “Meta uses this hashed information and compares it to [Meta’s] own hashed information to build custom audiences or more accurately determine which people took action in response to your ad.”<sup>62</sup>

71. Technological advances, including “the newest hardware (CPU and GPU) improvements” allow ordinary individuals to “decrypt SHA256.”<sup>63</sup>

72. However, even without access to the newest hardware technology, an ordinary person can reverse-engineer a SHA 256-encrypted code. Multiple free online resources allow even an ordinary person to generate and use SHA 256 encryptions. The following screenshot depicts a free online resource that allows individuals to encode any text into SHA 256.<sup>64</sup> Notably, the name input into the field labeled “Input value” contains the same name as the first name that Defendant disclosed to Meta, “Elizabeth.” The resulting hashed name,

<sup>60</sup> See Reference, META, <https://developers.facebook.com/docs/meta-pixel/advanced/advanced-matching>.

<sup>61</sup> See About hashing customer information, META BUSINESS HELP CENTER, <https://www.facebook.com/business/help/112061095610075?id=2469097953376494>.

<sup>62</sup> *Id.*

<sup>63</sup> SHA 256 CALCULATOR, <https://xorbin.com/tools/sha256-hash-calculator> (last accessed Oct. 20, 2023); see also *id.* (explaining that SHA 256 is historically a one-way cryptographic hash function, which is akin to a signature for a set of data).

<sup>64</sup> Sha 256 Generator, <https://tools.keycdn.com/sha256-online-generator>.

“b54f08623ae4039f55bcecb4961037fb4513d2ba9cb2b0667c5db970ac94911,” is the exact same as the one Defendant disclosed to Meta in the “udff [fn]” field as caught in Plaintiff’s counsel’s Website dynamic analysis.

## SHA256 Generator

GENERATE A SHA256 HASH

Input value

elizabeth

Generate

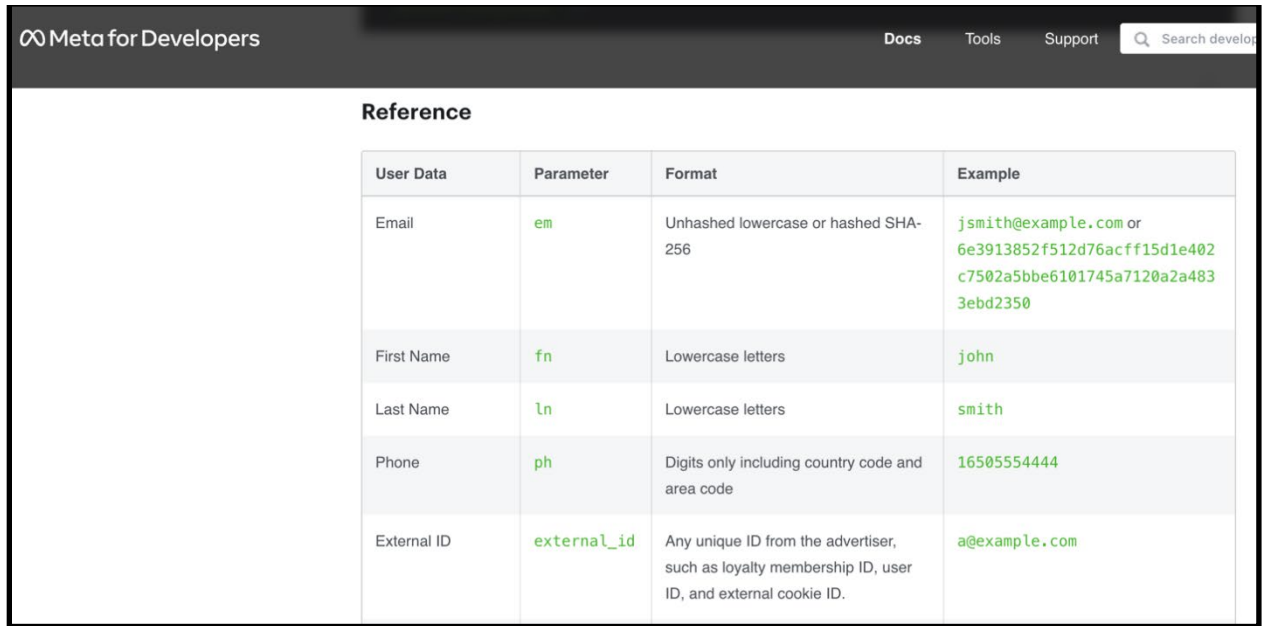
SHA256 HASH

b54f08623ae4039f55bcecb4961037fb4513d2ba9cb2b0667c5db970ac94911

73. Meta acknowledges that advertisers such as Defendant transmit users’ PII including, but not limited to, e-mail addresses and last names, on its Developers website. Specifically, Meta’s Reference sheet states that “em” stands for “e-mail,” and “fn” refers to a user’s first name.<sup>65</sup>

---

<sup>65</sup> See Reference, META, <https://developers.facebook.com/docs/meta-pixel/advanced/advanced-matching>.



The screenshot shows the 'Meta for Developers' documentation page. At the top, there are navigation links for 'Docs', 'Tools', and 'Support', along with a search bar. The main content is a 'Reference' section containing a table with the following data:

User Data	Parameter	Format	Example
Email	em	Unhashed lowercase or hashed SHA-256	jsmith@example.com or 6e3913852f512d76acff15d1e402 c7502a5bbe6101745a7120a2a483 3ebd2350
First Name	fn	Lowercase letters	john
Last Name	ln	Lowercase letters	smith
Phone	ph	Digits only including country code and area code	16505554444
External ID	external_id	Any unique ID from the advertiser, such as loyalty membership ID, user ID, and external cookie ID.	a@example.com

74. **Sprig.** Testing revealed that Defendant discloses Website users' PII in the form of email address, first name, and Sprig User ID to Sprig via the Sprig SDK. The following screenshot from the dynamic analysis captures the user's email address and first name being disclosed to Sprig:

```
email: blimalamamama@gmail.com
full_name: elizabeth
```

75. In addition, Defendant also disclosed to Sprig via the Sprig SDK a user's User ID (highlighted in pink in the screenshot below). As mentioned above, this unique string of letters, numbers, and hyphens identifies a specific user.

```
urn:com.mheducation.openlearning:enterprise.identity
:prod.us-east-1:person:86a694cb-e0eb-4c0d-956c-f1aca
19567b1
```

76. **Braze.** Testing revealed that Defendant similarly disclosed to Braze through the Braze SDK Website users' PII in the form of email address, first name, and User ID. The following screenshots are demonstrative:

```
DD', 'selected_title': 'Engineering Me
'email': 'blimalamamama@gmail.com'}
```



```
'full_name': 'elizabeth',
```

```
attributes: {'user_id':
'urn:com.mheducation.openlearning:enterprise.identity:prod.us-east-1:person:86a694cb-e0eb-4c0d-956c-f1aca
19567b1': 'custom': {'platform': 'web', 'id':
```

77. The User ID remains consistent in each of Defendant’s disclosures to Meta, Sprig, and Braze, making it likely that Defendant provides each of these third parties with backend tools to identify users by their User ID, among other characteristics. These third parties can use the User ID to further identify unique individual users and accordingly enhance Defendant’s marketing, advertising, and analytics processes of its user base.

v. *Defendant Discloses Information Identifying Which Specific Videos Were Watched By Which Specific Website Users To Meta, Sprig, And Braze*

78. The dynamic analysis captured Defendant disclosing the name of pre-recorded videos Website users watched, as well as the video ID of the pre-recorded video watched by any given user, in addition to whether the user actually watched that video to Meta, Sprig, and Braze through their respective SDKs and the Meta Tracking Pixel.

79. **Meta.** The dynamic analysis captured Defendant disclosing a user’s video-viewing information in the form of video title, video ID, and whether a user actually began to play the video to Meta through the Meta Tracking Pixel. The video’s name is populated in the field called “cd[ activity\_name ],” and the video ID is populated in the field called “cd[ content\_id ].” The field labelled “ev,” which stands for event, states that the user began playing the video. The following screenshots capture this:

```
cd[activity_id]: 01H7CRDVKMSSAYJPPH5R93KCSE
cd[activity_name]: Vectors: Force and Position
cd[activity_type]: OVERVIEW
cd[activity_length]: 1
cd[activity_content_position]: 0
cd[concept_id]:
cd[concept_name]:
cd[activity_content_type]: overview_video
cd[content_id]: 01H7CRDYCJKZR5DARYJNW30YKQ
cd[video_length_seconds]: 0
```

```
id: 756577239011030
ev: Video Started
d1:
```

80. **Sprig.** The dynamic analysis captured Defendant disclosing a users' video-viewing information in the form of video name, video ID, and whether a user played the video to Sprig through the Sprig SDK. The following screenshots are demonstrative:

```
activity_name: Vectors: Force and Position
```

```
content_id: 01H7CRDYCJKZR5DARYJNW30YKQ
```

```
event: Video Started
```

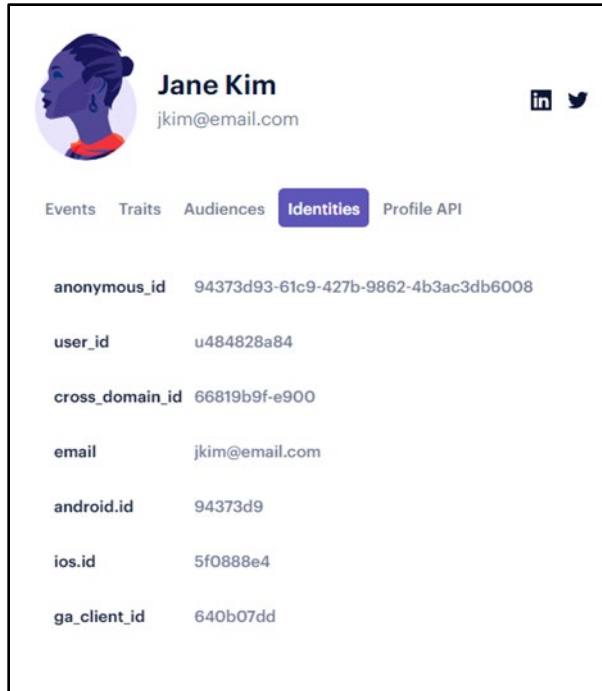
81. **Braze.** Finally, the dynamic analysis also captured Defendant disclosing a user's video-viewing information in the form of video name, video ID, and whether a user played the video to Braze through the Braze SDK.

```
'e': 'Vectors: Force and Position', 'activi  
_content_position': 0, 'concept_id': '', '  
'content_id': '01H7CRDYCJKZR5DARYJNW30YKQ'
```

```
{'n': 'Video Finished',
```

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

82. **Twilio.** As the dynamic analysis established, when a user watches a video on the App, Defendant discloses users' email addresses and full names to Twilio via the Segment SDK, along with video-viewing information such as the video title, video ID, and video interactions. Defendant discloses personally identifiable information to Twilio so Twilio can help Defendant with marketing, advertising, and analytics. As alleged above, the Segment SDK is designed to analyze user data from the App, aid in marketing campaigns, conduct targeted advertising, and ultimately boost Defendant's revenue.



83. Twilio entices developers to integrate the Segment SDK by underscoring its signature feature: “Engage.” Formerly known as “Personas,” Engage “is a powerful personalization platform that helps you create unified customer profiles.”<sup>66</sup> Twilio creates these “unified customer profiles” by “tak[ing] event data from across devices and channels and intelligently merg[ing] it into complete user- or account-level profiles.”<sup>67</sup>

84. Twilio builds these personas through “Segment Identity Resolution.” This process “merges the complete history of each customer into a single profile, no matter where they interact with your business.”<sup>68</sup> The Segment Identity Resolution supports, among other identifiers, “cookie IDs, device IDs, emails, and custom external IDs,” helping Twilio capture “a user’s interaction

<sup>66</sup> Engage Introduction, TWILIO, <https://segment.com/docs/engage/>.

<sup>67</sup> *Id.*

<sup>68</sup> Personas Identity Resolution Overview, TWILIO, <https://segment.com/docs/personas/identity-resolution/#:~:text=The%20Segment%20Identity%20Graph%20merges,they%20interact%20with%20your%20business.>

across web, mobile, server and third party partner touch-points in real-time[.]”<sup>69</sup> The Segment Identity Resolution then combines these “multiple external IDs,” into “one persistent ID,”<sup>70</sup> culminating into its offered Engage consumer profile.

85. In short, Defendant utilizes the Segment SDK to 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 its App, and maximize revenue by collecting and disclosing as much PII as possible to Twilio via the Segment SDK.

86. **Sprig.** Defendant discloses a user’s PII including email address, first name, User ID, and video-viewing information in the form of video title, video ID, and video interactions to Sprig so that Sprig’s “product experience platform” can “empower [Defendant] to fuel product growth with AI insights.”<sup>71</sup>

87. Sprig offers twenty-three different products that “bring user insights into every step of [Defendant’s] product development.”<sup>72</sup> The plethora of integrations Sprig offers allows customers like Defendant to “Leverage [their] customer data for enhanced targeting,” “Share user insights for seamless team collaboration,” and “Make product decisions with quantitative & qualitative data ... to understand how to solve” “pain points” in “user journeys.”<sup>73</sup>

88. Defendant uses Sprig’s multitude of technological offerings to assist in its marketing, analytics, and advertising functions for its Website.

---

<sup>69</sup> *Id.*

<sup>70</sup> *Id.*

<sup>71</sup> About Sprig, SPRIG, <https://docs.sprig.com/docs/what-is-sprig>.

<sup>72</sup> Integrate Sprig across your entire tech stack, SPRIG, <https://sprig.com/integrations#analytics>.

<sup>73</sup> *Id.*

89. *Meta.* Defendant discloses a user’s PII including name, email address, User ID, and video-viewing information in the form of video title, video ID, and video interactions to Meta so that Meta can “personali[ze] content, tailor[] and measur[e] ads, and provid[e] a safer experience.”<sup>74</sup>

90. The Meta Pixel allows Defendant “to track [its] website visitors’ actions,” which Meta calls conversion tracking.<sup>75</sup> “Tracked conversions ... can be used to analyze [Defendant’s] return on ad investment.”<sup>76</sup>

91. Notably, “[e]ach time the Pixel loads, it automatically ... track[s]” and records the URL that a Website user viewed.<sup>77</sup> In other words, so long as Defendant has installed the Meta Tracking Pixel onto the Website, anyone who views that webpage—meaning all Website users—“will be tracked using that” automatic URL tracker.<sup>78</sup> And, as mentioned above, the tracked URL discloses to Meta the exact video(s) that a Website user views. 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.”<sup>79</sup>

92. “Once tracked, custom conversions”—such as the URL tracking tool—“can be used to optimize [Defendant’s] ad campaigns”<sup>80</sup> through other Meta tools such as Ads Insights.<sup>81</sup>

---

<sup>74</sup> Cookies Policy, META, [https://www.facebook.com/privacy/policies/cookies/?entry\\_point=cookie\\_policy\\_redirect&entry=0](https://www.facebook.com/privacy/policies/cookies/?entry_point=cookie_policy_redirect&entry=0).

<sup>75</sup> Conversion Tracking, META, <https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking>.

<sup>76</sup> *Id.*

<sup>77</sup> Custom Conversions, META, <https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking#custom-conversions>.

<sup>78</sup> *Id.*

<sup>79</sup> *Id.*

<sup>80</sup> *Id.*

<sup>81</sup> Custom Conversions Insights, META, <https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking#custom-conversions>.

93. Defendant utilizes Meta’s comprehensive array of tracking and analytics tools to optimize its marketing, advertising, and analytics.

94. **Braze.** Defendant discloses a user’s PII including name, email address, User ID, and video-viewing information in the form of video title, video ID, and video interactions to Braze so that Braze can “[m]aximize the value of [Defendant’s] tech stack,” “[p]ersonalize every interaction,” and “[r]each the right audience.”<sup>82</sup>

95. Through the specific technological tools Braze offers, such as “Data Collection” and the creation of “User Profile[s],” “track[ing] ... user actions” and associating user actions with collected data, then analyzing the data in various dashboards, reports, and the Braze AI, Defendant is able to amplify its marketing, analytics, and advertising processes.

96. Defendant uses the features of the Braze SDK in Defendant’s integration of the Braze SDK into Defendant’s Website to analyze user data, create and analyze the performance of marketing campaigns, and target specific users or specific groups of users for advertisements. All of this helps Defendant further monetize the Website and maximize revenue by collecting and disclosing as much PII as possible to Braze via the Braze SDK.

#### **D. Defendant Knowingly Discloses Its Users’ PII To The Third Parties**

97. Based on the above, it is abundantly clear that Defendant *intentionally* and *knowingly* discloses to third parties, including Twilio, Meta, Sprig, and Braze, through their respective SDKs its users’ personally identifiable information and video-viewing information.

98. To further demonstrate that Defendant is intentionally and knowingly disclosing users’ PII to third parties, Defendant’s Privacy Policy<sup>83</sup> states “McGraw Hill uses your PII to

---

<sup>82</sup> Braze Data Platform, BRAZE, <https://www.braze.com/product/braze-data-platform>.

<sup>83</sup> The iOS App Store’s Sharpen App has a privacy policy link that leads to Defendant’s Website privacy policy. The current Customer Privacy Policy on Defendant’s website was updated on June 18, 2024. Plaintiff cites to the previous version of the Customer Privacy Policy on Defendant’s website, which was in effect from May 18, 2021. This older version is available through the

provide you with materials that we believe are of interest. ... McGraw Hill shares your information with third parties to provide you with marketing from us.”<sup>84</sup>

99. Specifically, Defendant states that “[w]hen you visit or make transactions on our web sites, we automatically collect certain information from you through the use of cookies, web beacons or other tracking mechanisms. ... This [information] allows McGraw Hill to collect information about customer usage and online behavior to tailor marketing to areas that may be more appropriate for the customer.”<sup>85</sup> Defendant’s privacy policy also states that it retains users’ PII for an undisclosed amount of time under the McGraw Hill data retention policies.<sup>86</sup>

100. Moreover, common sense dictates that a sophisticated content producer like Defendant, who includes multiple SDKs in its App and Website that are focused on marketing, advertising, and analytics, is fully aware of the scope of the data that those SDKs are collecting and is choosing to intentionally provide that data to the third-party SDK providers that it partners with.

#### **IV. PLAINTIFF’S EXPERIENCE**

101. On or about October 2023, Plaintiff Harwell created a Sharpen account and downloaded the Sharpen iOS App. Around the same time, Plaintiff also accessed the Sharpen Website through his Sharpen account.

102. From approximately October 2023 to December 2023, Plaintiff Harwell used his iPhone to access Sharpen videos through his account on the iOS Sharpen App. From

---

Wayback Machine at the network address: <https://web.archive.org/web/20231129082439/https://www.mheducation.com/privacy.html?ot-policy=customer>.

<sup>84</sup> McGraw Hill Customer Privacy Notice, MCGRAW HILL (May 18, 2024), <https://web.archive.org/web/20231129082439/https://www.mheducation.com/privacy.html?ot-policy=customer>. Defendant also defines PII to include not only “name[s]” and “location data,” but also “an identification number ... [or] an online identifier” such as a User ID. *See id.*

<sup>85</sup> *Id.*

<sup>86</sup> *See id.*

approximately October 2023 to December 2023, Plaintiff Harwell also used the Website to access Sharpen videos through his account. During that time, Plaintiff regularly used his account on the Sharpen App and Website to play pre-recorded videos.

103. At all relevant times, Plaintiff Harwell never consented, agreed, or otherwise permitted the App and Website to disclose his PII to third parties.

104. Likewise, Defendant never gave Plaintiff Harwell the opportunity to prevent the App and Website from disclosing his PII to third parties.

105. Nevertheless, each time Plaintiff Harwell accessed a video on the App, Defendant disclosed his PII to Twilio via the Segment SDK in the forms of his name, email, User ID, along with the title of the video he requested, the video's ID, and his interactions with that video. With this information, Twilio was given the ability to identify Plaintiff and attribute his video viewing records to his individualized profile maintained in its database. Indeed, even ordinary people could use the data disclosed to Twilio to identify Plaintiff. Critically, Plaintiff's PII was used to add to, create, or improve the efficacy of marketing and advertising analytics specific to Plaintiff, based on his activity in Defendant's App.

106. In addition, each time Plaintiff Harwell accessed a video on the Website, Defendant disclosed his PII to Meta, Sprig, and Braze via the Meta Tracking Pixel, the Sprig SDK, and the Braze SDK respectively. To Meta, Defendant disclosed Plaintiff's first name, (hashed) email address, fbp identifier, and User ID as well as his video viewing information in the form of video title, video ID, and video interactions. To Sprig, Defendant disclosed Plaintiff's first name, email address, and User ID as well as his video viewing information in the form of the video title, video ID, and video interactions. And to Braze, Defendant disclosed Plaintiff's first name, email address, and User ID as well as Plaintiff's video viewing information in the form of video title, video ID, and video interactions. With this information, Meta, Sprig, and Braze were each given the ability



to identify Plaintiff and attribute his video viewing records to his individualized profile maintained in each third party's respective database. Indeed, even an ordinary person could use the data Defendant disclosed to Meta, Sprig, and Braze to identify Plaintiff and the videos he viewed on the Website. Critically, Plaintiff's PII was used to add to, create, or improve the efficacy of marketing and advertising analytics specific to Plaintiff, based on his activity in Defendant's Website.

### **CLASS ALLEGATIONS**

107. **Class Definition.** Plaintiff seeks to represent a class of similarly situated individuals defined as all persons in the United States who made a Sharpen account, viewed a pre-recorded video on the App or Website, and had their PII transmitted to a third party (the "Class").

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

109. **Numerosity (Fed. R. Civ. P. 23(a)(1)):** At this time, Plaintiff does not know the exact number of members of the aforementioned Class. However, given the popularity of the App and Website, the number of persons within the Class is believed to be so numerous that joinder of all members is impractical.

110. **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 Class that predominate over questions that may affect individual members of the Class include:

- (a) Whether Defendant collected Plaintiff's and the Class' PII;
- (b) Whether Defendant unlawfully disclosed and continues to disclose its users' PII, including their video viewing records, in violation of the VPPA;
- (c) whether Defendant's disclosures were committed knowingly; and

- (d) whether Defendant disclosed Plaintiff's and the Class' PII without consent.

111. **Typicality (Fed. R. Civ. P. 23(a)(3)):** Plaintiff's claims are typical of those of the Class because Plaintiff, like all members of the Class, watched videos on the App and had his PII collected and disclosed by Defendant to third parties.

112. **Adequacy (Fed. R. Civ. P. 23(a)(4)):** Plaintiff has retained and is represented by qualified and competent counsel who are highly experienced in complex consumer class action litigation, including litigation concerning the VPPA and its state-inspired offspring. Plaintiff and his counsel are committed to vigorously prosecuting this class action. Moreover, Plaintiff is able to fairly and adequately represent and protect the interests of the Class. Neither Plaintiff nor his counsel have any interest adverse to, or in conflict with, the interests of the absent members of the Class. Plaintiff has raised viable statutory claims, of the type reasonably expected to be raised by members of the Class and will vigorously pursue those claims. If necessary, Plaintiff may seek leave of this Court to amend this Class Action Complaint to include additional representatives to represent the Class, additional claims as may be appropriate, or to amend the definition of the Class to address any steps that Defendant took.

113. **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 Class is impracticable. Even if every member of the Class 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 Class. Plaintiff anticipates no difficulty in the management of this action as a class action.

**COUNT I**  
**Violation of the VPPA**  
**18 U.S.C. § 2710**

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

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

116. 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, or 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 videos (*i.e.*, “similar audio visual materials” under the VPPA’s definition) to consumers via the App.

117. Plaintiff and members of the Class are “consumers” as defined by the VPPA because they downloaded, installed, and watched videos using the App. 18 U.S.C. § 2710(a)(1). Under the VPPA, therefore, Plaintiff and members of the Class are “subscribers” of “goods or services from a video tape service provider.” 18 U.S.C. § 2710(a)(1); *see also Yershov v. Gannett Satellite Information Network, Inc.*, 820 F.3d 482, 487-89 (1st Cir. 2016).

118. Plaintiff and members of the Class viewed videos using the App and Website. During these occasions, the App and Website disclosed Plaintiff’s and members of the Class’ PII. Specifically, Plaintiff’s and Class Members’ full names, email addresses, and the video titles of the videos watched by Plaintiff and Class Members were disclosed to third parties through the Segment SDK, Sprig SDK, Braze SDK, and Meta Pixel.

119. Defendant’s transmission of Plaintiff’s and Class Members’ PII to the forementioned third parties via SDKs constitutes a “knowing[] disclosure[]” of Plaintiff’s and members of the Classes’ “personally identifiable information” to a person as proscribed by the VPPA. 18 U.S.C. § 2710(a)(1).

120. 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 the Defendant constitutes “personally identifiable information” because it allows even an ordinary person to identify Plaintiff and members of the Class, as well as which specific videos were watched by Plaintiff and the Class. The disclosures also make it “reasonably and foreseeably likely to reveal” which specific videos were obtained by each Plaintiff and each member of the Class.

121. Plaintiff and members of the Class did not provide Defendant with any form of consent—either written or otherwise—to disclose their PII to third parties. 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, Sprig, Meta, and Braze were not necessary for “debt collection activities, order fulfillment, request processing, [or] transfer of ownership.” 18 U.S.C. § 2710(a)(2).

122. On behalf of himself 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 and costs and other litigation expenses.

**PRAYER FOR RELIEF**

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

- (a) For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure, naming Plaintiff as the representative of the Class, and naming Plaintiff's attorneys as Class Counsel to represent the Class;
- (b) For an order declaring that Defendant's conduct violates the statutes referenced herein;
- (c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;
- (d) For 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 injunctive relief as pleaded or as the Court may deem proper; and
- (h) For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and costs of suit.

**JURY TRIAL DEMANDED**

Plaintiff demands a trial by jury on all claims so triable.

Dated: September 24, 2024

Respectfully submitted,

**BURSOR & FISHER, P.A.**

By: /s/ Yitzchak Kopel  
Yitzchak Kopel

Yitzchak Z. 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  
Email: ykopel@bursor.com  
mroberts@bursor.com  
vzhou@bursor.com

*Attorneys for Plaintiff*