IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

JANIELLE DAWSON, individually and on behalf of others similarly situated,

Plaintiff,

v.

THE UNIVERSITY OF PHOENIX, INC.,

Defendant.

Case No. 1:25-cv-03497

Judge Mary M. Rowland

MEMORANDUM OPINION AND ORDER

Plaintiff Janielle Dawson ("Plaintiff" or "Dawson"), on behalf of herself and all others similarly situated, brings this putative class action suit against the University of Phoenix, Inc. ("Defendant" or "the University") for allegedly disclosing her video-watching behavior and educational records to third-parties through Defendant's use of third-party tracking technologies without Plaintiff's consent. Plaintiff asserts violations of (a) the Video Privacy Protection Act ("VPPA"), 18 U.S.C. § 2710; (b) the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2510, *et seq*.; and (c) the Illinois Eavesdropping Act, 720 Ill. Comp. Stat. 5/1, *et seq*. Defendant moved to dismiss Plaintiff's putative class action complaint for failure to state a claim under Federal Rule of Civil Procedure 12(b)(6). [19], [20].[1] For the reasons stated herein, Defendant's Motion to Dismiss is granted in part and denied in part.

[1] In addition to Defendant's and Plaintiff's memoranda, the Court also considered numerous supplemental authorities submitted by the parties. [28]–[32], [36]–[37], [39]–[40], [42]–[45], [47], [50].

I. Background

The following factual allegations taken from the operative complaint ([1]) are accepted as true for the purposes of the motion to dismiss. *See Lax v. Mayorkas*, 20 F.4th 1178, 1181 (7th Cir. 2021).

Defendant University of Phoenix is an online post-secondary education institution that offers courses taught through prerecorded videos. [1] ¶¶ 12, 73. In 2016, Plaintiff Janielle Dawson enrolled in a degree program with the University of Phoenix to obtain a Bachelor of Science Degree in Business. *Id.* ¶ 4. Since enrolling, Plaintiff has purchased and enrolled in numerous classes offered by Defendant. *Id.* ¶¶ 4–5. In connection with her coursework, Plaintiff views prerecorded videos, obtains and turns in assignments, communicates with faculty, takes tests, views her transcript and grades, and pays for courses and tuition through the University's website. *Id.* ¶ 6. Unbeknownst to Plaintiff, every time she accessed Defendant's website, tracking technology offered by Meta Platforms, Inc. ("Facebook"), Google LLC ("Google"), LinkedIn Corporation ("LinkedIn"), ByteDance ("TikTok"), Microsoft Corporation ("Microsoft"), and Amazon.com, Inc. ("Amazon") were running in the background. *Id.* ¶ 8. Plaintiff alleges Defendant used the tracking technologies offered by Facebook and other third-parties to: (a) disclose Plaintiff's video-watching behavior and other personally identifiable information, to Facebook and the other third-parties; and (b) allow the third-parties to intercept and obtain Plaintiff's confidential education records protected from disclosure by the Family Educational Rights and Privacy Act ("FERPA"). *Id.*

The complaint explains the technologies employed by each of the third-party companies. *Id.* at ¶¶ 26–72. The Court focuses here on Facebook as an example. Facebook is the world's largest social networking site that generates revenue, at least in part, by selling advertising space on its website. *Id.* ¶¶ 26–27. To effectively target advertisements, Facebook tracks its users' activity on and off its website. *Id.* ¶ 28. "Core Audiences" is Facebook's generalized dataset of user data that advertisers can use to apply specialized parameters for their targeted advertisements. *Id.* Advertisers may also develop "Custom Audiences" to target "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." *Id.* ¶ 29. Advertisers who utilize "Custom Audiences" must supply the underlying data to Facebook either by manually uploading contact information for their customers or by using Facebook's "Business Tools" that collect and transmit data automatically, including the Facebook Tracking Pixel. *Id.*

The Facebook Tracking Pixel tracks people and their actions on websites employing the Pixel. *Id.* ¶ 30. More specifically, when a user accesses a website hosting the Facebook Tracking Pixel, Facebook's software script surreptitiously directs the user's browser to send a separate message to Facebook's servers concurrent with the communications with the host website all without the user's knowledge. *Id.* This separate transmission, initiated by Facebook code, contains the original GET request sent to the host website, along with additional data that the Facebook Tracking Pixel is configured to collect. *Id.* "Two sets of code are thus

automatically run as part of the browser's attempt to load and read Defendant's websites—Defendant's own code and Facebook's embedded code." *Id.* After Facebook receives the record, the company processes it, analyzes it, and assimilates it into datasets like the Core Audiences and Custom Audiences for the advertiser and for Facebook's own purposes, such as improving its advertising network and machine-learning algorithms. *Id.* ¶¶ 32–33. Advertisers, like Defendant, control what actions the Facebook Tracking Pixel collects and how the Pixel identifies visitors. *Id.* ¶¶ 34–35.

Plaintiff alleges the Facebook Tracking Pixel monitors when students purchase a degree program or a single course and each step of the enrollment process on Defendant's website. ¶¶ 74–75. When a student who is logged into Facebook purchases and enrolls in a degree program or course on the University's website, the Facebook Tracking Pixel transmits PageView data, including information about the degrees and courses a student purchased, from the Facebook cookies to Facebook along with the person's PageView data. *Id.* ¶¶ 76, 78.

Name	Value	Domain
ar_debug	1	.facebook.com
fr	1KEhqGgEzfNpxflcd.AWWjyaQZRp2...	.facebook.com
c_user	679395441	.facebook.com
dpr	1.5	.facebook.com
ps_l	1	.facebook.com
xs	27%3AasgrOb2ovNSlPQ%3A2%3A...	.facebook.com
sb	_MvhZhEX7ZeI9FAjN0dTN-n5	.facebook.com
datr	9cvhZr5vG9HVMmQsnsSuW_aP	.facebook.com
ps_n	1	.facebook.com
wd	1707x791	.facebook.com

For instance, the c_user cookie in the code above contains a visitor's Facebook ID. *Id.*

¶¶ 77–78. Plaintiff alleges a Facebook ID is personally identifiable information because anyone can identify a Facebook profile—and all personal information publicly listed on that profile—by appending the Facebook ID to the end of facebook.com. *Id.* ¶ 79. By combining the PageView data and personally identifiable information from Facebook cookies on the University website, Facebook can see students' video-watching behavior. *Id.* ¶ 80. Plaintiff contends the University discloses and allows the interception of students' data and communications to generate increased profits by (a) targeted advertisements that are based on students' video-watching behavior, education records; and (b) improved course offerings. *Id.* ¶ 84.

Plaintiff asserts Defendant's conduct violates the Video Privacy Protection Act, 18 U.S.C. § 2710, *et seq.* ("VPPA"); the Electronic Communications and Privacy Act, 18 U.S.C. § 2510, *et seq.* ("ECPA"); and the Illinois Eavesdropping Act, 720 Ill. Comp. Stat. 5/14-1, *et seq*. Defendant moves to dismiss all three counts.

II. Standard

"To survive a motion to dismiss under Rule 12(b)(6), the complaint must provide enough factual information to state a claim to relief that is plausible on its face and raise a right to relief above the speculative level." *Haywood v. Massage Envy Franchising, LLC*, 887 F.3d 329, 333 (7th Cir. 2018) (quoting *Camasta v. Jos. A. Bank Clothiers, Inc.*, 761 F.3d 732, 736 (7th Cir. 2014)); *see also* Fed. R. Civ. P. 8(a)(2) (requiring a complaint to contain a "short and plain statement of the claim showing that the pleader is entitled to relief"). A court deciding a Rule 12(b)(6) motion

"construe[s] the complaint in the light most favorable to the plaintiff, accept[s] all well-pleaded facts as true, and draw[s] all reasonable inferences in the plaintiff's favor." *Lax*, 20 F.4th at 1181. However, the court need not accept as true "statements of law or unsupported conclusory factual allegations." *Id.* (quoting *Bilek v. Fed. Ins. Co.*, 8 F.4th 581, 586 (7th Cir. 2021)). "While detailed factual allegations are not necessary to survive a motion to dismiss, [the standard] does require 'more than mere labels and conclusions or a formulaic recitation of the elements of a cause of action to be considered adequate.'" *Sevugan v. Direct Energy Servs., LLC*, 931 F.3d 610, 614 (7th Cir. 2019) (quoting *Bell v. City of Chicago*, 835 F.3d 736, 738 (7th Cir. 2016)).

Dismissal for failure to state a claim is proper "when the allegations in a complaint, however true, could not raise a claim of entitlement to relief." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 558 (2007). Deciding the plausibility of the claim is "a context-specific task that requires the reviewing court to draw on its judicial experience and common sense." *McCauley v. City of Chicago*, 671 F.3d 611, 616 (7th Cir. 2011) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009)).

III. Analysis

A. Video Privacy Protection Act

In Count I, Plaintiff asserts Defendant violates the Video Privacy Protection Act ("VPPA"). [1] ¶¶ 97–105. Congress enacted the VPPA in response to a profile of then-Supreme Court nominee Judge Robert H. Bork that was published by a Washington, D.C., newspaper during his confirmation hearings. S. Rep. No. 100–599, at 5 (1988), *reprinted in* 1988 U.S.C.C.A.N. 4342–1. The profile contained a list of

films that Judge Bork and his family had rented from a video store, thus causing members of Congress to denounce the disclosure as repugnant to the right of privacy. *Id.* at 5–8. Consequently, Congress passed the VPPA "[t]o preserve personal privacy with respect to the rental, purchase or delivery of video tapes or similar audio visual materials." *Id.* at 1.

To state a claim under the VPPA, a plaintiff must allege the defendant (1) is a video tape service provider ("VTSP"); (2) who knowingly disclosed to any person; (3) personally identifiable information ("PII"); (4) concerning any consumer without her consent. *See* 18 U.S.C. § 2710(b)(1), (b)(2). The University contends Plaintiff has failed to allege the required elements, including actual damages. [20] at 2–9. The University also argues the VPPA is unconstitutional. *Id.* at 9–14. Plaintiff contests Defendant's arguments. The Court addresses each issue in turn.

i. Video Tape Service Provider

The parties dispute whether Plaintiff adequately has pleaded that the University is a VTSP as defined by the VPPA. [20] at 2–4. Defendant argues delivering video materials is not the focus of the University's work, and thus, the University does not meet the statutory definition of a VTSP. [20] at 2 (citing *In re Vizio, Inc., Consumer Priv. Litig.*, 238 F. Supp. 3d 1204, 1221–22 (C.D. Cal. 2017)). The Court disagrees.

The VPPA defines a VTSP as "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).

This definition is "broad" and "cast[s] a wide net." *Salazar v. Nat'l Basketball Ass'n*, 118 F.4th 533, 548 (2d Cir. 2024) (explaining the definition of VTSP under the VPPA in the context of analyzing the meaning of "goods or services").[2] VTSP "is not limited to entities that deal exclusively in audiovisual content; rather, audiovisual content need only be *part* of the provider's book of business." *Id.* (emphasis in original). Allegations that a defendant regularly delivers video content is sufficient to plausibly plead a defendant is a VTSP. *See, e.g.*, *Manza v. Pesi, Inc.*, 784 F. Supp. 3d 1110, 1114 (W.D. Wis. 2025) (holding plaintiff adequately alleged provider of continuing education for mental health professionals is a VTSP where a "primary feature of [defendant's] website is the sale of prerecorded video courses and seminars on various healthcare topics"); *In re Facebook Inc. Cons. Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 799 (N.D. Cal. 2019) (denying motion to dismiss VPPA claim and finding it is plausible to conclude Facebook is a VTSP from allegations that Facebook "'regularly delivers' video content to users and maintains a cache of videos and visual materials, including from content providers like Netflix, for their delivery to users").

Here, Plaintiff plausibly avers that Defendant is a VTSP. Plaintiff alleges Defendant is an online university that "sells degree programs and single courses." [1] ¶ 73. The University teaches its programs and courses, at least in part, by using prerecorded video lectures. *Id.*; *see also id.* ¶ 99 ("Defendant delivers and sells prerecorded videos to University of Phoenix students"). Plaintiff claims her class courses routinely included prerecorded videos, which she viewed in connection with

[2] The Seventh Circuit has yet to speak directly on what constitutes a "video tape service provider."

completing her coursework on the University's website. *Id.* ¶¶ 7, 102. Nothing further is needed at this stage. Plaintiff plausibly alleges that the University of Phoenix is a video tape service provider because it "engages in the business" of delivering videos.

Defendant's arguments to the contrary are unavailing. First, Defendant asserts it is not "engaged in the business" of delivering audio visual materials because its videos are ancillary to its core business, which is providing post-secondary education. [20] at 2–3. Courts that have considered what it means to be "engaged in the business of" delivering videos have explained "for the defendant to be engaged in the business of delivering video content, the defendant's product must not only be substantially involved in the conveyance of video content to consumers but also significantly tailored to serve that purpose." *In re Vizio, Inc.*, 238 F. Supp. 3d at 1221 (contrasting a letter carrier who physically places a package containing a videotape into a consumer's mailbox with a television manufacturer who installs applications for consumers to access video programming on its televisions). At least one court in this District has rejected this exact theory in a case with similar factual circumstances. *Krueger v. Chess.com, LLC*, 2025 WL 2765375, at *3–4 (N.D. Ill. Sept. 28, 2025) (concluding plaintiff sufficiently alleged website focused on delivering videos of chess matches and lessons to its users was "engaged in the business" of delivering videos despite argument that videos were ancillary to the core business). So too here.

Contrary to the cases cited by Defendant, Plaintiff's allegations support the reasonable inference that the University provides videos as more than a peripheral

part of its marketing strategy or brand awareness. *Goodman v. Hillsdale College*, 2025 WL 2941542, at *5 (W.D. Mich. Oct. 17, 2025) ("[N]othing in the VPPA limits liability to entities that *primarily* distribute videos. Rather, video tape service provider is defined broadly to include even those businesses that dabble in video rentals.") (internal quotation omitted). *Cf. Banks v. CoStar Realty Info., Inc.*, 2025 WL 2959228, at *3–5 (E.D. Mo. Oct. 20, 2025) (apartment tour videos are not comparable to prerecorded video cassette tapes and realty company was in the business of connecting property owners and renters, not to deliver prerecorded videos); *Rodriguez v. Delta T LLC*, 2023 WL 9419152,*4 (C.D. Cal. Dec. 12, 2023) (videos on how to assemble, wire, and install ceiling fans are a marketing tool and by including such videos on its website, defendant is not engaged in the business of delivering video content); *Cantu v. Sunrun Inc.*, 2023 WL 11795670, *3 (S.D. Cal. Nov. 22, 2023) (solar company's marketing videos are not the company's product or main focus of its endeavors); *Cantu v. Tapestry, Inc.*, 2023 WL 4440662, *8–10 (S.D. Cal. Jul. 10, 2023) (handbag retailer's business was not significantly tailored to consumers watching videos on retailer's sales website); *Carroll, et al., v. General Mills, Inc.*, 2023 WL 4361093 at *3–4 (C.D. Cal. Jun. 26, 2023) (videos on food manufacturer's websites were a part of the defendant's brand awareness and defendant's business is not focused on providing video content).[3] The University's

[3] Other cases cited by Defendant are inapposite. In *Osheske v. Silver Cinemas Acquisition Co.*, 132 F.4th 1110 (9th Cir. 2025), the Ninth Circuit concluded the defendant movie theater was not a VTSP because the Act does not encompass the provision of shared access to film screenings. 132 F.4th at 1113. Unlike the theater, which did not engage in the "rental, sale, or delivery" of video content because there was no transaction involving an exchange of video materials, Plaintiff and other class members purchase video courses from the University. *Compare id. with* [1] ¶¶ 7, 102. And in *Pileggi v. Washington Newspaper Publ'g Co., LLC*, 146 F.4th 1219 (D.C. Cir. 2025), the D.C. Circuit affirmed the

prerecorded videos are not used to advertise other products, but instead the prerecorded lecture videos are the product that the University's business is tailored to disseminate.

Next, Defendant posits a parade of unconvincing horribles. It argues finding the University is a VTSP "would convert every school which has ever shown videos to its students as part of their coursework into a 'video tape service provider.'" [20] at 3. That is not what is alleged here. Plaintiff here took entire courses via pre-recorded video. Finally, Defendant asserts concluding the University is not a VTSP is consistent with the legislative history since the impetus of the legislation was the publication of the video titles then-Supreme Court nominee Judge Robert Bork and his family rented from a video rental store. *Id.* at 4. But the language of the statute controls the meaning of the legislation, *Gardner v. Me-TV Nat'l Ltd. P'ship*, 132 F.4th 1022, 1025 (7th Cir. 2025), and the language of the VPPA supports this Court's determination that Plaintiff has plausibly pleaded that the University is a VTSP.

ii. Consumer

Defendant contends Plaintiff failed to plead she is a "consumer" under the VPPA. [20] at 4–5. A "consumer" is defined as "any renter, purchaser, or subscriber of goods or services from a video tape service provider." 18 U.S.C. § 2710(a)(1). Defendant argues it is absurd to conclude that students who pay tuition to enroll and attend school are within the same definitional category as renters, purchasers, or

dismissal of the complaint on the basis that plaintiff failed to allege she was a consumer within the meaning of the VPPA and did not reach the definition of VTSP. 146 F.4th at 1237. The concurrence in *Pileggi* limited VTSPs to physical objects, which contravenes the prevailing body of caselaw addressing this issue as discussed above. *Id.* at 1239.

subscribers. [20] at 4. Additionally, Defendant claims a post-secondary degree is not a good or service. *Id.* at 4–5. Although Defendant references numerous dictionary definitions, it does not explain how those definitions are incompatible with the VPPA nor does it cite any legal authority to support its arguments. *See id.*

The Seventh Circuit addressed the meaning of "consumer" under the VPPA and determined "when a person does furnish valuable data in exchange for benefits, that person becomes a 'consumer.'" *Gardner*, 132 F.4th at 1025.[4] It reasonably follows the same is true when a user exchanges monetary value, such as tuition payments, in exchange for benefits. Here, Plaintiff alleges she purchased and enrolled in a degree program, including numerous courses, at the University. [1] ¶¶ 4–6, 100, 102. Those allegations sufficiently support a claim that Plaintiff is a consumer within the meaning of the VPPA.

iii. Personally Identifiable Information

The VPPA prohibits a VTSP from "knowingly disclos[ing], to any person, personally identifiable information concerning any consumer of such provider" without the consumer's informed consent. 18 U.S.C. § 2710(b). The VPPA does not expressly define personally identifiable information ("PII"), but provides PII "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).

Plaintiff alleges the University installed and embedded tracking technology

[4] Other circuits have adopted a narrower interpretation of "consumer." *See, e.g.*, *Salazar v. Paramount Glob.*, 133 F.4th 642, 651 (6th Cir. 2025) (linking "goods and services" to "audio visual materials"). Plaintiff, who alleges she viewed prerecorded lecture videos, also qualifies as a consumer within this interpretation of the term. *See* [1] ¶¶ 7, 102.

from third-parties into its website, phoenix.edu, which Plaintiff accessed to view prerecorded videos and other activities related to her enrollment. [1] ¶¶ 1, 6. Whenever Plaintiff accessed phoenix.edu, the website ran tracking technology from third-parties, including Facebook, Google, LinkedIn, ByteDance, Microsoft, and Amazon, that allegedly sent data regarding Plaintiff's video-watching alongside identifying information. *Id.* ¶¶ 8, 74–84. For example, the Facebook Tracking Pixel runs on Defendant's website and sends students' enrolled course information and Facebook ID, which is a sequence of numbers assigned only to that Meta accountholder, to Facebook. *Id.* ¶¶ 74–80. Plaintiff alleges other third-party companies with tracking technology running on Defendant's website operate similarly. *Id.* ¶¶ 81–83. Plaintiff contends this data can be used by third-party technology companies to identify Defendant's students and what videos students accessed and viewed on Defendant's website. *Id.* ¶¶ 80, 101. According to Plaintiff, both the University and third-parties use this data to target their advertising and increase profits. *Id.* ¶¶ 33, 42, 44, 54, 59, 69, 71–72, 84, 120. Accordingly, Plaintiff claims this data constitutes PII and Defendant's disclosure violated the VPPA. *Id.* ¶¶ 101, 103–4.

Defendant argues Plaintiff does not plausibly allege the data disclosed to third-party companies constitutes personally identifiable information within the meaning of the statute. [20] at 6–7. According to Defendant, Plaintiff's allegations are limited to static digital identifiers that, when viewed by an ordinary person, do not identify that person. *Id.* at 7. For example, Defendant claims a Facebook ID "does not *alone*

identify anyone to a reasonable person, but rather must be combined with other data such as whatever information may be available on a public Facebook profile." [27] at 4. Plaintiff disputes that the ordinary person standard applied by Defendant is proper and instead advocates for the application of a different standard of reasonable foreseeability. [23] at 6–9. Even if the ordinary person standard is correct, Plaintiff contends she adequately pleaded that an ordinary person could use the data disclosed, such as Facebook ID numbers, to identify her. *Id.*

Neither the Supreme Court nor the Seventh Circuit have addressed the meaning of PII under the VPPA. Courts that have analyzed this question recognize the Act lacks clarity. *See, e.g.*, *Yershov v. Gannett Satellite Info. Network, Inc.*, 820 F.3d 482, 486 (1st Cir. 2016) ("The statutory term "personally identifiable information" is awkward and unclear"); *In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262, 281 (3d Cir. 2016) ("what counts as personally identifiable information under the Act is not entirely clear"); *see also Solomon v. Flipps Media, Inc.*, 136 F.4th 41, 48 (2d Cir. 2025) ("the VPPA is not well drafted") (cleaned up); *Sterk v. Redbox Automated Retail, LLC*, 672 F.3d 535, 538 (7th Cir. 2012) ("[t]he statute is not well drafted").

Although that statutory language is far from clear, there is no dispute among reviewing courts that the Act contemplates more than information that explicitly names an individual person and identifies the videos she obtained. *See Yershov,* 820 F.3d at 486; *Solomon*, 136 F.4th at 51–52; *In re Nickelodeon*, 827 F. 3d at 290; *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 984 (9th Cir. 2017). Rather, PII includes

information that *can be used* to identify an individual. *Eichenberger*, 876 F.3d at 984. The plain language of the VPPA's text supports this interpretation. If Congress intended a narrower construction, it could have inserted appropriate language in the provision to render their intention obvious. *Hall v. United States*, 566 U.S. 506, 523 (2012) ("if Congress intended that result, it did not so provide in the statute . . . it is not for us to rewrite the statute"). Congress chose not to do so.

Instead, Congress used the open-ended word "includes." 18 U.S.C. § 2710(a)(3). This word typically indicates that the proffered definition is not exclusive or exhaustive. *See Sauk Prairie Conservation All. v. United States Dep't of the Interior*, 944 F.3d 664, 671 (7th Cir. 2019) ("we generally read the word 'including' to 'introduce[ ] examples, not an exhaustive list.'") (quoting *Bernal v. NRA Grp., LLC*, 930 F.3d 891, 894 (7th Cir. 2019)). The other VPPA statutorily defined terms use the word "means" to define them in contrast to "includes" here, further supporting that Congress intended a broader meaning. *Compare* 18 U.S.C. § 2710(a)(3) (using the word "includes") *with* 18 U.S.C. § 2710(a)(1), (a)(2) & (a)(4) (using the word "means" to define other statutory terms).[5]

Furthermore, as explained in *Eichenberger*, Congress's use of the word "identifiable" adds meaning. 18 U.S.C. § 2710(a)(3). The suffix "able" means "capable of." *Able*, Merriam-Webster.com, https://www.merriam-webster.com/dictionary/able (last visited Oct. 27, 2025). Accordingly, PII includes information that is "capable of" identifying a person, not just information that, standing alone, identifies a person.

[5] The congressional record is in accord. S. Rep. No. 100-599, at 12 (1988) (stating that the drafters' aim was "to establish a minimum, but not exclusive, definition of personally identifiable information").

Concluding otherwise would defy common sense and allow a VTSP to skirt liability by disclosing information other than names that readily can be used to identify a consumer.

Thus, the question for the Court is whether the University's disclosures (numeric identifications tied to video watching and Facebook IDs, along with other data) can be used to identify a particular person who viewed certain videos. The Circuits that have considered this question are split as to how to interpret this provision—specifically regarding *who* will use the information to identify a consumer.[6] The Second, Third, and Ninth Circuits have adopted an "ordinary person" test. *Solomon*, 136 F.4th at 51–54 (concluding disclosure of computer code, which included plaintiff's Facebook ID was not PII because it is implausible an ordinary person could identify the video name and Facebook ID from the transmitted computer code); *In re Nickelodeon*, 827 F.3d at 290 (holding disclosure of a user's IP address, a user's browser and operating system settings, and computing device's unique device identifier did not readily permit an ordinary person to identify a specific individual's watched videos); *Eichenberger*, 876 F.3d at 985 (concluding disclosure of Roku device serial number where third-party would need to be combine the data with information in its sole possession did not constitute PII). The ordinary person standard, as first articulated by the Third Circuit, assesses whether the disclosed information "would,

[6] Despite annunciating two coherent standards, the circuits that have addressed this question minimize the difference. *In re Nickelodeon*, 827 F.3d at 289 (finding no split with the First Circuit and describing PII as a spectrum); *Eichenberger*, 876 F.3d at 986 ("Our decision today, though it adopts a different test, does not necessarily conflict with *Yershov*. . . . [M]odern technology may indeed alter—or may already have altered—what qualifies under the statute. A Facebook link or an email address may very well readily enable an 'ordinary person' to identify an individual.").

with little or no extra effort, permit an ordinary recipient to identify a particular person's video-watching habits." *In re Nickelodeon*, 827 F.3d at 284. The ordinary person standard, as adopted by in *Solomon*, "effectively shut the door for Pixel-based VPPA claims" in the Second Circuit. *Hughes v. Nat'l Football League*, 2025 WL 1720295, at *2 (2d Cir. June 20, 2025). In contrast, the reasonable foreseeability standard adopted by the First Circuit focuses on whether the disclosed "information reasonably and foreseeably [is] likely to reveal which" videos the customer viewed. *Yershov*, 820 F.3d at 486 (finding disclosure of unique Android ID and the GPS coordinates of the plaintiff's device that a third-party used to link the videos viewed to an individualized profile maintained by the third-party amounted to a disclosure connecting the plaintiff to the viewed videos).

The Court finds it unnecessary to choose either approach because the result is the same under both tests.[7] A Facebook ID is sufficient for an ordinary person to identify a specific person, and is reasonably and foreseeably likely to reveal a specific person. Facebook describes itself as a "real identity platform," meaning users are allowed only one account and must share "the name they go by in everyday life." [1]

[7] Although the Court need not endorse either the "ordinary person" standard or the "reasonable foreseeability" standard, the Court recognizes the persuasive analysis in *Manza v. Pesi, Inc.*, 784 F. Supp. 3d 1110 (D. Wis. 2025), the only case in the Seventh Circuit to opine on the appropriate standard for PII under the VPPA. There, the court adopted the reasonably foreseeable test and observed "[t]he courts that have adopted the 'ordinary person' standard have identified little textual basis for the limitation they impose." *Id.* at 1119. The ordinary person standard has been justified because the VPPA requires a defendant "knowingly disclose, is sufficient for an ordinary person to identify a specific person, and is reasonably and foreseeably likely to reveal" but where a "defendant knows that the recipient of the disclosure can readily use the information to determine a user's identity, the knowledge requirement is satisfied regardless of whether the ordinary person standard is met." *Goodman*, 2025 WL 2941542, at *8.

¶ 26. Accordingly, when creating an account, users must provide their first and last name, along with their birthday and gender. *Id.* An ordinary person need only add an individual's Facebook ID number to "Facebook.com/" to generate that individual's Facebook profile, which in turn contains an individual's name and other information. In other words, unlike static digital identifiers, it is unnecessary to combine the Facebook ID with other information in the exclusive possession of a third-party or to conduct an additional investigation to discover an individual's identity. *Cf. Eichenberger*, 876 F.3d at 986 (disclosure of a Roku device serial number "*cannot* identify an individual unless it is combined with other data in [a third-party]'s possession"); *In re Nickelodeon*, 827 F.3d at 286 (disclosure of static digital identifiers such as IP addresses did not violate the VPPA because they only revealed the identify of a particular computer and not a person).

On this issue, the Second Circuit's application of the ordinary person standard in *Solomon* is unpersuasive.[8] Based on 29 lines of exemplar computer code, the court concluded it was implausible that an ordinary person could decipher the titles of videos watched or identify an individual's Facebook ID when that text is "interspersed with many characters, numbers, and letters." *Solomon*, 136 F.4th at 54. But it is nonsensical to categorize information as PII based on its format, rather than the type of information conveyed. *See Cole v. LinkedIn Corp.*, 2025 WL 2963221, at *6 (N.D. Cal. Oct. 20, 2025) ("Nothing in the statute suggests that a defendant can

[8] Decisions in the Second Circuit applying *Solomon* are similarly unpersuasive for the same reason. *See, e.g.*, *Nixon v. Pond5, Inc.*, 2025 WL 2030303, at *4–5 (S.D.N.Y. July 21, 2025); *Golden v. NBCUniversal Media, LLC*, 2025 WL 2530689, at *5–7 (S.D.N.Y. Sept. 3, 2025); *Taino v. Bow Tie Cinemas, LLC*, 2025 WL 2652730, at *7–8 (S.D.N.Y. Sept. 16, 2025).

escape liability by disclosing such information in a format that makes it less likely that an ordinary person receiving the information would actually use it to identify an individual's video-watching behavior."); *Goodman*, 2025 WL 2941542, at *8. "The Facebook User ID is more than a unique, anonymous identifier. It personally identifies a Facebook user. That it is a string of numbers and letters does not alter the conclusion. Code is a language, and languages contain names, and the string is the Facebook user name." *In re Hulu Priv. Litig.*, 2014 WL 1724344, at *14 (N.D. Cal. Apr. 28, 2014). More than nonsensical, such a system would create a significant loophole in the VPPA that would allow VTSPs to evade liability by formatting PII into code. *Manza*, 784 F. Supp. 3d at 1122. The information included in the exemplar in the complaint is plainly sufficient for an ordinary person, or Meta, to determine a person's Facebook ID. *See* [1] ¶ 77.

Courts across the country routinely hold Facebook IDs are PII pursuant to the VPPA. *See, e.g.*, *Lee v. Springer Nature Am., Inc.*, 769 F. Supp. 3d 234, 261 (S.D.N.Y. 2025) (collecting cases) ("Courts have generally recognized that Facebook IDs constitute PII under the VPPA."); *Ghanaat v. Numerade Labs, Inc.*, 689 F. Supp. 3d 714, 720 (N.D. Cal. 2023) (collecting cases) ("Most, if not all, courts to address the question have found at the pleading stage that Facebook IDs are PII.") (footnote omitted); *Braun v. Philadelphia Inquirer, LLC*, 2023 WL 7544160, at *4 (E.D. Pa. Nov. 13, 2023) (same); *Martinez v. D2C, LLC*, 2023 WL 6587308, at *4 (S.D. Fla. Oct. 10, 2023) (quoting *Sellers v. Bleacher Rep., Inc.*, 2023 WL 4850180, at *4 (N.D. Cal. July 28, 2023)) ("The [Facebook ID] is a unique identifier that is enough, on its own,

to identify a person."). Even the *In re Nickelodeon* court acknowledged that something like a Facebook ID could be sufficient to state a claim. *See* 827 F.3d at 290 ("Some disclosures predicated on new technology, such as . . . customer ID numbers, may suffice.").

Other courts have reached the same conclusion—that a Facebook ID constitutes PII regardless of whether the ordinary person or reasonably foreseeable standard applies. *See, e.g.*, *Goodman*, 2025 WL 2941542, at *8 (expressing disagreement with *Solomon*); *Haines v. Cengage Learning, Inc.*, 2025 WL 2336089, at *8 (S.D. Ohio May 5, 2025), *report and recommendation adopted*, No. 1:24-CV-710, 2025 WL 2045644 (S.D. Ohio July 22, 2025) (noting *Solomon* is "in stark contrast to the vast majority of federal district and circuit courts that have held the opposite about a Facebook ID") (internal quotation omitted); *Feldman v. Star Trib. Media Co. LLC*, 659 F. Supp. 3d 1006, 1021 (D. Minn. 2023). And other courts have determined that a Facebook ID constitutes PII under just the ordinary person standard. *See, e.g.*, *Cole*, 2025 WL 2963221, at *5–6; *Plotsker v. Envato Pty Ltd.*, 2025 WL 2481422, at *7–8 (C.D. Cal. Aug. 26, 2025).

In sum, Plaintiff has sufficiently alleged that the University disclosed her personally identifiable information to Facebook. As to the remaining third-party technology companies that purportedly tracked pixels and ran cookies on the University's website, the Court agrees with Defendant—Plaintiff's allegations are too conclusory to support a claim. *See* [20] at 6. There are insufficient allegations that the information disclosed to Google, LinkedIn, TikTok, Microsoft, and Amazon

plausibly identify Plaintiff and other class members. [1] ¶¶ 47 ("Google uses IP addresses and unique device identifiers to track internet users"); 48–50 ("browser fingerprinting" techniques employed by Google can "identify 99.24 percent of all users"); 54 (LinkedIn "collects data on a website visitor including the URL, referrer, IP address, and device and browser characteristics") (internal quotations omitted); 64 (TikTok collects metadata, button clicks, timestamps for digital events, and a visitor's IP address); 71 (Microsoft collects "Machine Unique Identifiers" from users); 72 (alleging Amazon's software code operates similar to that of Facebook, Google, LinkedIn, TikTok, and Microsoft). At most, these static digital identifiers identify a computer or device, not a person. *In re Nickelodeon*, 827 F.3d at 286

Defendant claims Plaintiff did not plausibly allege the University "knowingly disclosed" PII because Plaintiff does not allege the University knew whether she or other class members had a Facebook account much less that the University knew her Facebook ID. [20] at 7. But Plaintiff alleges that "Defendant knowingly disclosed Plaintiff's PII, as defined by the VPPA, because it knowingly installed the tracking technologies of the Third-Party Tracking Companies on the Website" and "Defendant utilized the tracking technologies offered by the Third-Party Tracking Companies to compel Plaintiff's and Class members' web browsers to transfer Plaintiff's and Class members' identifying information, like their Facebook IDs, along with Plaintiff's and Class members' event data, including information about the videos they viewed." [1] ¶¶ 101, 103. That is sufficient. *See, e.g.*, *Cole*, 2025 WL 2963221, at *6 ("allegation that LinkedIn knowingly installed the Pixel and configured it in a manner resulting

in the conveyance of her personally identifiable information to third parties sufficiently pleads that LinkedIn knowingly disclosed her personally identifiable information"); *Sellers*, 2023 WL 4850180, at *5 (allegations that defendant "deliberately installed the Facebook pixel on its website . . . to improve its targeted advertising and increase its revenue" were "enough for the court to reasonably infer that defendant knowingly discloses personally identifying information.").

iv. Actual Damages

Under the VPPA, a court may award "actual damages but not less than liquidated damages in an amount of $2,500." 18 U.S.C. 2710(c). Here, Defendant argues Plaintiff is not entitled to statutory damages under the VPPA because she "has not alleged any actual damages." [20] at 7–9. In support of this theory, Defendant relies on *Doe v. Chao*, 540 U.S. 614 (2004). There, the Supreme Court interpreted the following provision from the Privacy Act of 1974: "[if the United States violates the Privacy Act], the United States shall be liable to the individual in an amount equal to the sum of actual damages sustained by the individual…but in no case shall a person entitled to recovery receive less than the sum of $1,000." *Id.* at 619 (quoting 5 U.S.C. § 552a(g)(4)(A)). The Court concluded that actual damages are a prerequisite to recovering the statutory amount. *Id.* at 627.

The only court to directly address this issue distinguished *Chao* and held the VPPA does not condition recovery on proof of actual damages. *Saunders v. Hearst Television, Inc.*, 711 F. Supp. 3d 24, 31–32 (D. Mass. 2024). *Saunders* explained the Supreme Court noted in *Chao* that "if Congress wished to allow recovery of liquidated

damages for violations of the Privacy Act absent actual damages, it could have made the statute read 'the Government would be liable to the individual for actual damages 'but in no case . . . less than the sum of $1,000.'" *Id.* at 32 (quoting *Chao*, 540 U.S. at 623). "That is nearly exactly how the VPPA is styled." *Id.*; *see* 18 U.S.C. § 2710(c)(2)(A) ("The court may award actual damages but not less than liquidated damages in an amount of $2,500.").

The Court adopts the reasoning and conclusion in *Saunders*. Plaintiff may proceed without alleging any specific pecuniary loss. *See Sterk*, 672 F.3d at 538 ("True, subsection (c)(2)(A) allows $2,500 in 'liquidated damages,' without need to prove "actual damages") (dictum); *In re Hulu Priv. Litig.*, 2013 WL 6773794, at *10 (N.D. Cal. Dec. 20, 2013) (explaining "[t]he similarities between the [Drivers Privacy Protection Act} and the VPPA support the same conclusion" that the VPPA "permits an award of liquidated damages without proof of actual damages").

v. Constitutionality of the VPPA

Finally, the University contends the VPPA imposes severe speech restrictions that burden free speech and cannot be justified in violation of the First Amendment. [20] at 9–14. The parties dispute the appropriate level of scrutiny with which the Court should review the statute. Defendant asserts strict scrutiny applies to this constitutional analysis because the VPPA is a content- and speaker-based regulation of speech, but that the Court need not decide the level of scrutiny because the Act cannot even pass First Amendment muster under the lesser intermediate scrutiny standard. *Id.* Plaintiff responds that intermediate scrutiny is appropriate here for

two independent reasons: the University's speech is commercial in nature and the VPPA is content-neutral. [23] at 11–14. Plaintiff argues the Act is consonant with the First Amendment. *Id.*

As a preliminary matter, this Court must determine whether to apply strict or intermediate scrutiny. The First Amendment prohibits the enactment of laws "abridging the freedom of speech." U.S. Const., Amdt. 1. This means "that government has no power to restrict expression because of its message, its ideas, its subject matter, or its content." *Police Dept. of Chicago v. Mosley*, 408 U.S. 92, 95 (1972). "Content-based laws—those that target speech based on its communicative content—are presumptively unconstitutional." *Reed v. Town of Gilbert, Ariz.*, 576 U.S. 155, 163 (2015). Such content-based laws "may be justified only if the government proves that they" satisfy strict scrutiny. *Id.* In a similar vein, "[l]aws designed or intended to suppress or restrict the expression of specific speakers contradict basic First Amendment principles." *United States v. Playboy Ent. Grp., Inc.*, 529 U.S. 803, 812 (2000).

But "not all speech is of equal First Amendment importance." *Snyder v. Phelps*, 562 U.S. 443, 452 (2011) (quoting *Hustler Magazine, Inc. v. Falwell*, 485 U.S. 46, 56 (1988)). Accordingly, courts have recognized that some categories of speech do not warrant strict scrutiny even if regulated based on content. *Stark v. Patreon, Inc.*, 656 F. Supp. 3d 1018, 1027 (N.D. Cal. 2023). For example, "restrictions on protected expression are distinct from restrictions on economic activity." *Sorrell v. IMS Health, Inc.*, 564 U.S. 552, 567 (2011). Consequently, "the First Amendment does not prevent

restrictions directed at commerce or conduct from imposing incidental burdens on speech." *Id.* Commercial speech is subject to a test under intermediate scrutiny. *Fla. Bar v. Went For It, Inc.*, 515 U.S. 618, 623 (1995); *Adams Outdoor Advert. Ltd. P'ship v. City of Madison, Wisconsin*, 56 F.4th 1111, 1116 (7th Cir. 2023).

"To determine whether speech falls on the commercial or noncommercial side of the constitutional line, the [Supreme] Court has provided this basic definition: Commercial speech is 'speech that proposes a commercial transaction.'" *Jordan v. Jewel Food Stores, Inc.*, 743 F.3d 509, 516 (7th Cir. 2014) (quoting *Bd. of Trs. of State Univ. of New York v. Fox*, 492 U.S. 469, 482 (1989) (emphasis removed)); *see also Briggs & Stratton Corp. v. Baldrige*, 728 F.2d 915, 917–18 (7th Cir. 1984) (the "hallmark of commercial speech" is that it "pertains to commercial transactions"). But this core "definition is just a starting point." *Jordan*, 743 F.3d at 516. Other relevant guideposts and considerations for classifying speech that contains both commercial and noncommercial elements are "(1) the speech is an advertisement; (2) the speech refers to a specific product; and (3) the speaker has an economic motivation for the speech." *United States v. Benson*, 561 F.3d 718, 725 (7th Cir. 2009) (*Bolger v. Youngs Drug Products Corp.*, 463 U.S. 60, 66–67 (1983)). "This is just a general framework, however; no one factor is sufficient, and *Bolger* strongly implied that all are not necessary." *Jordan*, 743 F.3d at 517; *see also Bolger*, 463 U.S. at 67 n.14 ("Nor do we mean to suggest that each of the characteristics present in this case must necessarily be present in order for speech to be commercial.").

The *Bolger* factors do not produce a clear outcome here. Defendant's alleged

disclosure of Plaintiff's and other student class members' information to third-party technology companies are not advertisements in a traditional sense, though they allegedly informed the placement of advertisements. *See, e.g.*, [1] ¶ 28 (alleging that "Facebook can target users so effectively because it surveils user activity both on and off its site" using the Facebook Tracking Pixel). Although the disclosure did not refer to a particular product as an advertisement ordinarily might, it referred to the video products that Plaintiffs viewed, and Plaintiff's personally identifiable information is arguably itself a product in the information ecosystem in which companies like Facebook and Defendant operate. *See Gardner*, 132 F.4th at 1024 ("In an Information Age, data can be worth more than money."). As for economic motivation, Plaintiff has alleged that both the University and third-party companies were motivated to derive economic gain from building better profiles of their users for the purpose of targeting their products. [1] ¶¶ 33 (alleging "Facebook benefits from the information it collects from its clients' websites, such as Defendant's students who visit the Website, because Facebook uses this information to improve its advertising network, including its machine-learning algorithms and its ability to target users with ads"); 84 (alleging "Defendant discloses, and otherwise allows the interception, of the PII and communications described herein in order to generate increased profits by way of, *inter alia*: (a) targeted advertisements that are based on students' video-watching behavior, education records and other PII; and (b) improved course offerings"). There is no clear indication that either Defendant or the third-parties to this transfer of information had non-economic motivation.

Following the analysis another district court undertook when assessing the constitutionality of the VPPA, the Court takes a "wholistic approach" to assess the University's alleged transfer of Plaintiff's personally identifiable information and video viewing activity to third-parties. *See Stark*, 656 F. Supp. 3d at 1034; *Jordan*, 743 F.3d at 517 (explaining "there is a 'common-sense distinction' between commercial speech and other varieties of speech, and [the courts] are to give effect to that distinction") (quoting *Ohralik v. Ohio State Bar Ass'n*, 436 U.S. 447, 455–56 (1978)). Like in *Stark*, the challenged conduct here is a disclosure of Plaintiff's commercial interactions with Defendant, a student at a for-profit university who purchased classes. Both the University and third-party technology companies were motivated to more effectively sell or otherwise monetize their products, with no expressive or creative content beyond the fact of Plaintiff's personal information and interactions, containing nothing of public interest, and serving no non-economic purpose to either the speaker or the recipient. When viewing the disclosure as a whole, the Court finds that the University's alleged speech is commercial. *Cf. Stark*, 656 F. Supp. 3d at 1034 (noting "as is most similar speech governed by the VPPA in the context of corporate data collection and analysis").

Defendant's cases do not compel a different conclusion. Unlike the amended Telephone Consumer Protection Act of 1991 at issue in *Barr v. Am. Ass'n of Pol. Consultants, Inc.*, 591 U.S. 610 (2020), which impermissibly favored speech made for the purpose of collecting government debt over core First Amendment speech, such as political and other speech, thus having more than a mere effect on speech, the law

at issue here, which does not favor one type of speech over another, imposes only an incidental burden on the University's speech. 591 U.S. at 632; *see also id.* at 620 (noting *Barr* "is not intended to expand existing First Amendment doctrine or to otherwise affect traditional or ordinary economic regulation of commercial activity"). *Reed v. Town of Gilbert, Ariz.*, 576 U.S. 155 (2015) and *Dahlstrom v. Sun-Times Media, LLC*, 777 F.3d 937 (7th Cir. 2015) are similarly unavailing. Contrary to Defendant's assertions, the challenged regulation of advertising signs in *Reed* only targeted non-commercial speech. 576 U.S. at 159–61. And the *Dahlstrom* court did not address whether the prohibition on disclosure of motor vehicle records by newspaper reports constituted commercial speech. 777 F.3d at 949–54. Finally, in *Sorrell*, the Supreme Court determined the outcome was the same regardless of whether "a special commercial speech inquiry or a stricter form of judicial scrutiny [was] applied," and therefore did not decide what standard applied there. 564 U.S. at 571. These cases do not displace the longstanding principle that regulations of commercial speech may be subject to intermediate scrutiny even if content-based.[9]

As stated above, commercial speech is analyzed under intermediate scrutiny. *Fla. Bar*, 515 U.S. at 623; *Adams Outdoor Advert.*, 56 F.4th at 1116. Generally, a statute will survive intermediate scrutiny if it "advances important governmental interests unrelated to the suppression of free speech and does not burden

[9] Because the Court determines the regulated speech is commercial in nature and, as described below, withstands intermediate scrutiny, the Court need not determine whether the VPPA is content-based or content-neutral. Furthermore, speaker-based distinctions abound in state and federal privacy laws without violating the First Amendment. *Shapiro v. Peacock TV*, 2025 WL 968519, at *7 n.5 (S.D.N.Y. Mar. 31, 2025) (citing Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. § 1320d-9 (limiting applicability to "covered entit[ies]"); FERPA, 20 U.S.C. § 1232g(a) (limiting applicability to "educational agencies or institutions")).

substantially more speech than necessary to further those interests." *Turner Broad. Sys., Inc. v. F.C.C.*, 520 U.S. 180, 189 (1997). Commercial speech is governed by a test set forth in *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York*, 447 U.S. 557 (1980). Commercial speech that concerns lawful activity and is not misleading may be regulated if the government: (1) "assert[s] a substantial interest in support of its regulation"; (2) "demonstrate[s] that the restriction on commercial speech directly and materially advances that interest"; and (3) the regulation is "narrowly drawn." *Fla. Bar*, 515 U.S. at 624 (quoting *Cent. Hudson Gas & Elec. Corp.*, 447 U.S. at 564–65). The "fit between the legislature's ends and the means chosen to accomplish those ends [need] not necessarily [be] perfect, but reasonable." *Fox*, 492 U.S. at 480 (omitting quotes). The Court determines the VPPA satisfies the intermediate scrutiny test for commercial speech.

First, Congress stated a substantial interest in support of enacting the VPPA: "to preserve personal privacy with respect to the rental, purchase or delivery of video tapes or similar audio visual materials." S. Rep. 100-599 at 1. The legislative record reflects that Congress considered such privacy protections critical to safeguarding individual thought and intellectual growth and to avoid chilling such freedoms in fear of political surveillance, embarrassment, or conformity. *Id.* at 7–8. This is far from the "broad" and "sweeping assertions" of privacy Defendant claims it to be. [20] at 12; [27] at 7 (both citing *U.S. W., Inc. v. F.C.C.*, 182 F.3d 1224, 1234–35 (10th Cir. 1999)). To the contrary, the VPPA follows a long line of statutes extending privacy protection to records that contain information about individuals, S. Rep. 100-599 at 1, and the

Supreme Court has repeatedly recognized the sanctity of personal privacy. *Saunders*, 711 F. Supp. 3d at 33 (citing *Fla. Bar*, 515 U.S. at 625; *Frisby v. Schultz*, 487 U.S. 474, 483–485 (1988)). Furthermore, the VPPA integrates the findings and recommendations of the Privacy Protection Study Commission, thus the Act is based on meaningful evidence. *Contra Pac. Frontier v. Pleasant Grove City*, 414 F.3d 1221, 1235 n.12 (10th Cir. 2005) (finding anecdotes and common sense do not justify ordinance). Defendant also argues the VPPA constrains private speech rather than protecting First Amendment interests, seemingly urging the Court to jettison an individual's privacy interests in their video-watching data in favor of private VTSP's unbridled ability to disclose that private information. [20] at 12; [27] at 7. The Court is not persuaded.

Second, restricting the University from disclosing the videos that Plaintiff viewed alongside Plaintiff's PII to third-parties directly and materially advances the government's interest in protecting consumer privacy relating to the rental, purchase, or delivery of video materials. *Saunders*, 711 F. Supp. 3d at 33. Third, the court can conceive of no legitimate non-commercial First Amendment interest of the University that its exploitation of Plaintiffs' PII serves. *Saunders*, 711 F. Supp. 3d at 33. Finally, the VPPA is narrowly drawn because it applies only to a narrow group of business entities and specific group of consumers. *Id.*

Defendant contends the Act is impermissibly underinclusive because it only protects video-watching behavior but not books, magazines, photographs, course catalogs, or other student information; livestreamed content; certain video providers;

and certain users. [20] at 13–14; [27] at 8. "This is a difficult argument to make because 'the First Amendment imposes no freestanding 'underinclusiveness limitation.'" *Illinois Liberty PAC v. Madigan*, 904 F.3d 463, 470 (7th Cir. 2018) (*Williams-Yulee v. Fla. Bar*, 575 U.S. 433, 449 (2015)). The government "need not address all aspects of a problem in one fell swoop; policymakers may focus on their most pressing concerns." *Williams-Yulee*, 575 U.S. at 449. Courts routinely uphold laws—even under strict scrutiny—that conceivably could have restricted even greater amounts of speech in service of their stated interests. *Id.* Accordingly, the Court will not find the VPPA unconstitutional because it could have cast a wider net of protection and further burdened free speech. The Court finds the "fit" between Congress's goal of protecting privacy in this realm and its means to do so is at least reasonable. *See Fox*, 492 U.S. at 481.

In sum, the Court declines to find the VPPA is unconstitutional. This accords with the findings of other courts. *Saunders*, 711 F. Supp. 3d at 32–33 (finding the same); *IMDb.com Inc. v. Becerra*, 962 F.3d 1111, 1124 (9th Cir. 2020) (noting that statutes like the VPPA "regulate data collection and disclosure without implicating the First Amendment" (internal quotation marks omitted)); *Boehner v. McDermott*, 484 F.3d 573, 578 n.2 (D.C. Cir. 2007) (noting that disclosures may be lawfully constrained under the First Amendment, and citing the VPPA).

B. Electronic Communications Privacy Act

In Count II, Plaintiff asserts a claim for violations of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2510, *et seq*. [1] ¶¶ 106–27. The

ECPA provides for criminal and civil liability against anyone who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a); 18 U.S.C. § 2520. Defendant argues Plaintiff's ECPA claim fails for three reasons: (1) the ECPA is a one-party consent statute, and the University was a party to the communications; (2) the crime-tort exception to the party consent exception does not apply; and (3) the communications at issue were not intercepted "in transit." [20] at 15–20. Plaintiff disputes the one-party consent exception applies to her "procurement" theory of liability and argues she plausibly pleaded the communications at issue were intercepted "in transit." [23] at 14–21.

i. Mode of Liability and Crime-Tort Exception

First, Defendant argues the University, as the website owner who consented to implement the third-party tracking tools on its website, is a party to the communications at issue and that the ECPA does not impose liability on a person for intercepting communications when the person is a party to the alleged intercepted communications. [20] at 15–16 (citing 18 U.S.C. § 2511(2)(d)). Next, Defendant claims the crime-tort exception to the one-party consent exception is not available to Plaintiff because the exception does not apply to the interception itself. *Id.* at 16–19 (discussing 18 U.S.C. § 2511(2)(d)). Defendant contends Plaintiff has not pleaded a predicate criminal or tortious act separate and independent from the University's use of third-party tracking tools, and to the extent Plaintiff pleaded violations of VPPA and FERPA, she failed to state a claim. *Id.* Plaintiff concedes the University was a

party to the communications at issue, but contests that she alleged a violation of the ECPA via Defendant's direct interception of Plaintiff's communications. [23] at 18 n.3. Plaintiff states she alleged Defendant procured the third-party companies to intercept her communications. *Id.* at 15–18. Accordingly, Plaintiff insists Defendant's one-party consent exception and crime-tort exception to the exception arguments are moot. The Court will first address the viability of Plaintiff's "procurement" allegations.

Instead of direct interception, Plaintiff alleges the University violated the ECPA by "intentionally procur[ing] various third parties, including the Third-Party Tracking Companies, to intercept and endeavor to intercept the electronic communications of Plaintiff and Class members." [1] 1 ¶ 119; *see also id.* ¶ 121 ("Defendant knew and had reason to know that it procured the third parties to intercept the electronic communications at issue and used the fruits thereof in violation of the ECPA"). Defendant responds that the Court should dismiss Plaintiff's "procured" interception ECPA claim because, as Defendant argues, a civil action under § 2520 must be based on actual interception, disclosure, or use of a communication.[10] [27] at 9–10.

Courts are divided as to whether the ECPA provides for civil liability when a party procures third-parties to intercept communications. 18 U.S.C. § 2511(1)(a) states:

[10] Plaintiff also pleads Defendant violated the ECPA by unlawfully using and endeavoring to use the contents of Plaintiff's electronic communications to generate profits and increase revenues. [1] ¶ 120; *see also* [23] at 18–19. Defendant does not move to dismiss on this basis. *See* [20] at 14–19; [27] at 9–12.

> Except as otherwise specifically provided in this chapter any person who intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

This provision establishes criminal penalties for (a) intercepting wire, oral, or electronic communications; (b) endeavoring to intercept wire, oral, or electronic communications; and (c) procuring another person to intercept wire, oral, or electronic communications. § 2511 does not provide private civil causes of action or civil remedies, rather those rights are provided in § 2520 of the ECPA. Before the ECPA was amended in 1986, § 2520(a) read:

> Any person whose wire or oral communication is intercepted, disclosed, or used in violation of this chapter shall (1) have a civil cause of action against any person who intercepts, discloses, or uses or procures any other person to intercept, disclose, or use such communications, and (2) be entitled to recover from any such person.

Now, 18 U.S.C. § 2520(a) provides:

> any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

The clause "against any person who intercepts, discloses, or uses or procures any other person to intercept, disclose, or use such communications" was removed from the portion of the statute providing a civil remedy and replaced with "from the person or entity, other than the United States, which engaged in that violation." Language prohibiting the procurement of interception remained in the unamended underlying criminal statute, § 2511(1)(a).

In support of finding no civil cause of action for "procuring' interception of

communications, Defendant relies on non-binding and out-of-circuit precedent. [27] at 9–10. In *Peavy v. WFAA–TV, Inc.*, 221 F.3d 158 (5th Cir. 2000), the Fifth Circuit analyzed the plain text of the statute and concluded the 1986 amendment was intended to remove a civil cause of action against one who "procures" another to intercept communications. 221 F.3d at 168–69. Applying the rule that amendments to statutes are presumed meaningful, the Fifth Circuit concluded Congress intended to eliminate "procurement" liability from the ECPA. *Id.* at 169 (citing *Stone v. I.N.S.*, 514 U.S. 386, 397 (1995)). Some courts have followed the *Peavy* holding and limited "procurement" liability to criminal defendants. *See, e.g.*, *Kirch v. Embarq Management Co.*, 702 F.3d 1245, 1246–47 (10th Cir. 2012); *Council on Am.-Islamic Rels. Action Network, Inc. v. Gaubatz*, 891 F. Supp. 2d 13, 23–24 (D.D.C. 2012).

Yet other courts have reached a different conclusion when assessing the same language. Those courts reason that the 1986 amendment to § 2520(a) does not support limiting civil liability. *See, e.g.*, *Q.J. v. PowerSchool Holdings, LLC*, 2025 WL 2410472, at *6 (N.D. Ill. Aug. 20, 2025) (Alonso, J.); *Boseovski v. McCloud Healthcare Clinic, Inc.*, 2020 WL 68578, at *6 (E.D. Cal. Jan. 7, 2020); *Valentine v. WideOpen W. Fin., LLC*, 288 F.R.D. 407, 412 n.3 (N.D. Ill. 2012) (Chang, J.); *Lonegan v. Hasty*, 436 F. Supp. 2d 419, 428 (E.D.N.Y. 2006). This Court agrees. § 2520(a) permits that the person whose communications were intercepted, disclosed, or used in violation of the ECPA may recover from the person or entity that engaged in that violation. And under § 2511(1)(a), persons whose communications are intercepted include those persons whose communications were intercepted by a third-party who was procured

to do so by a defendant. Both the persons directly intercepting the communications and the persons who procured interception have violated the ECPA. It follows that the victim of the wiretap may sue any person or entity who engaged in the violation, including procuring interception. And here, Plaintiff has sufficiently alleged the University procured third-parties to intercept or endeavor to intercept Plaintiff's electronic communications. *See* [1] ¶¶ 119, 121.

Having determined that Plaintiff may lodge a civil claim for procurement liability, we turn to address whether the University may invoke the one-party consent exception. Defendant argues Plaintiff's ECPA theory of liability fails because the University was a party to the communications which it procured; thus the one-party consent rule applies and Plaintiff has not adequately pleaded the crime-tort exception. [27] at 10–12. Plaintiff responds the one-party consent exception is not available to individuals and entities that procure another to intercept communications. [23] at 17. Defendant's legal authorities do not support its conclusion that the one-party consent exception still applies where Plaintiff alleged the University procured the interception, and Plaintiff does not cite any conclusive legal authority in support of her position that one-party consent is inapplicable here. In the absence of clear authority, the Court nevertheless considers whether Plaintiff plausibly pleaded the crime-tort exception applies.[11]

[11] In *Q.J. v. PowerSchool Holdings, LLC*, 2025 WL 2410472, another court in this district made a similar observation: "At least one court has observed that the statutory language is at least fuzzy as to whether the party exception applies when the defendant is sued under a procurer theory, rather than as the party who intercepted the communications in question." *Id.* at *6 n.3 (citing *Mekhail v. North Memorial Health Care*, 726 F. Supp. 3d 916 (D. Minn. 2024)). In *Mekhail*, the court explained "the statute's plain language appears to support the interpretation that the party exception was drafted with active interceptors[, not party procurers and users of others' interceptions,] foremost in

At this stage, the Court finds it is at least plausible that the crime-tort exception to the one-party consent exception applies and thus declines to dismiss the case because the University was a party to the communications. Plaintiff alleged Defendant procured third-party entities for the purpose of intercepting communications and obtaining data from students and other users of the University's website despite being protected from disclosure by law. [1] ¶¶ 23–25, 78, 80, 84, 86–88. *Accord Q.J.*, 2025 WL 2410472, at *6 (collecting cases); *Stein v. Edward-Elmhurst Health*, 2025 WL 580556, at *3–6 (N.D. Ill. Feb. 21, 2025) (finding allegation of having the purpose to commit an act that violates HIPAA is sufficient to invoke the crime tort exception). Defendant may test this claim through discovery and at later phases of litigation.

ii. "In Transit"

Defendant also claims Plaintiff's ECPA claims fail because she has not plausibly alleged any information was intercepted "in transit" as opposed to merely acquired by a third-party from electronic storage. [20] at 19–20. Plaintiff and the Court disagree.

Here, Plaintiff alleges the Facebook Tracking Pixel "transmit[s] the data automatically" and that the transmission of intercepted communications to Facebook "is initiated by Facebook code *and concurrent with the communications with the host website*." [1] ¶¶ 29–30 (emphasis added); *see also id.* ¶ 31 ("Facebook causes the

mind." 726 F. Supp. 3d at 926. In *Q.J.* and *Mikhail*, the courts did not resolve the issue because both courts concluded the plaintiffs' claims survived dismissal even assuming the party exception applied. *Q.J.*, 2025 WL 2410472 at *6 n.3; *Mekhail*, 726 F. Supp. 3d at 926–28. So too here.

browser to secretly and concurrently duplicate the communication with the Website, transmitting it to Facebook's servers."). Defendant contends the allegations in the complaint lack a temporal component and asserts that a "second" transmission cannot occur at the same time as the initial transmission to the University. [27] at 13. That interpretation contorts the plain allegations in the complaint; the Court does not credit this reading.

The Court is satisfied that Plaintiff has plausibly alleged that the third-parties at issue intercept the communications in real time directly from the website visitors, *i.e.*, in transit. *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002) (""for a website such as [defendant's] to be 'intercepted' in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage" because "[t]his conclusion is consistent with the ordinary meaning of 'intercept,' which is 'to stop, seize, or interrupt in progress or course before arrival.'")).

Accordingly, the Court declines to dismiss Plaintiff's ECPA claim.

C. Illinois Eavesdropping Act

In Count III, Plaintiff claims the University violated Section 5/14-2(a)(3) of the Illinois Eavesdropping Act ("IEA"). [1] ¶¶ 128–41. The IEA establishes civil liability when a person or his principal eavesdrops by participating in five categories of prohibited conduct. 720 ILCS 5/14-2(a); 5/14-6. Relevant here, it is unlawful under the IEA to "knowingly and intentionally . . . intercept, record, or transcribe, in a surreptitious manner, any private electronic communication to which he or she is not a party unless he or she does so with the consent of all parties to the private electronic

communication." 720 ILCS 5/14-2(a)(3). A "private electronic communication" refers to "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system, when the sending or receiving party intends the electronic communication to be private under circumstances reasonably justifying that expectation." 720 ILCS 5/14-1(e). And "surreptitious" is defined under the IEA as "obtained or made by stealth or deceptions, or executed through secrecy or concealment." 720 ILCS 5/14-1(g). The statute provides for civil remedies to injured parties against the eavesdropper *and the eavesdropper's principal*, including actual and punitive damages. 720 ILCS 5/14-6 (emphasis added).

Defendant argues Plaintiff fails to state a claim under the IEA for two independent reasons. First, the University was a party to the challenged conduct and Section 5/14-2(a)(3) only applies to non-parties to private electronic communications. Second, Plaintiff has not pleaded compensable damages as required by the Illinois statute. The Court considers both grounds but in large part declines to dismiss Plaintiff's IEA claim.

i. Principal Liability

Defendant asserts the Illinois Eavesdropping Act claim fails because the subsection Plaintiff invoked only applies to non-parties to private electronic communications. [20] at 21–22. Plaintiff does not dispute that the University was a party to the communications at issue. [23] at 18 n.3. She alleges Defendant is liable

as a principal of the various third-parties that ran tracking technology on the University's website. [1] ¶ 139; [23] at 21–24. Accordingly, some of the cases Defendants rely on are inapposite because they do not involve principal liability. *See, e.g.*, *Hannant v. Culbertson*, 2025 WL 2413894, at *11 (C.D. Ill. Aug. 20, 2025); *Zak v. Bose*, 2019 WL 1437909 (N.D. Ill. Mar. 31, 2019).

As defined in the IEA, a "principal" is "any person who: (1) knowingly employs another who illegally uses an eavesdropping device in the course of such employment; or (2) knowingly derives any benefit or information from the illegal use of an eavesdropping device by another; or (3) directs another to use an eavesdropping device illegally on his or her behalf." 720 ILCS 5/14-1(c). Here, Plaintiff contends Defendant knowingly derives a benefit and information from the illegal use of the third-parties' tracking technologies that Defendant integrated, installed, and embedded into the University's website. [1] ¶ 139. Further, Plaintiff alleges the University directed third-parties to illegally use an eavesdropping device on Defendant's behalf. *Id.*

Defendant disputes that the University can be considered a principal. The University argues because Section 5/14-2(a)(3) does not create civil liability for the actions of a party to private electronic communication, then it has not engaged in any "illegal" conduct. [27] at 14. But the plain language of the statute makes it clear that it is not that principal's use of an eavesdropping device but the third-parties' illegal use of an eavesdropping device that is at issue. 720 ILCS 5/14-1(c). Here, Plaintiff has plausibly alleged the third-parties running tracking technology on the University's

website are not parties to her communications with the University and the third-parties' computer codes and programs were "used to intercept, monitor, capture, and record Plaintiff's and Illinois Subclass members' communications and data transmissions while they were accessing and navigating the Website." [1] ¶ 138(a). Thus, Plaintiff has adequately alleged a violation of 720 ILCS 5/14-2(a)(3) and an illegal use of an eavesdropping device by the third-parties.

The Court also finds Plaintiff has alleged sufficient facts that the University "knowingly derive[d] a[ ] benefit or information from the illegal use of an eavesdropping device by another." 720 ILCS 5/14-1(c)(2). Plaintiff claims the University discloses and allows the interception of personally identifiable information and communications to generate increased profits by way of "(a) targeted advertisements that are based on students' video-watching behavior, education records and other PII; and (b) improved course offering." [1] ¶ 84. Accordingly, Defendant can plausibly be considered the principal that earned increased profit ("derive[d] a benefit") from the use of cookies and tracking technology ("eavesdropping device") on Defendant's website by third-parties ("by another"). However, the Court determines Plaintiff's conclusory allegations that Defendant directed third-parties to illegally use an eavesdropping device on its behalf are insufficient to support a claim.

Other courts in this district have reached the same conclusion in similar factual circumstances. *See, e.g.*, *Kurowski v. Rush Sys. for Health*, 683 F. Supp. 3d 836, 853 (N.D. Ill. 2023) ("*Kurowski I*") (declining to dismiss IEA premised on principal liability involving plaintiff alleged health system non-consensually and

surreptitiously deployed third-party source code on its website and patient portal that transmitted patients' personally identifiable patient data to advertisers where the system profited from the interception).

Defendants remaining arguments fail for a variety of reasons. First, Defendant takes issue with Plaintiff's allegation that the University is an "eavesdropper" for two reasons: (1) the subsection of the Illinois *Eavesdropper* Act Plaintiff invokes, Section 5/14-2(a)(3), provides the elements of when "a person commits eavesdropping" does not include the word "eavesdropper;" and (2) the IEA defines an "eavesdropper" as a party to a "private conversation," which in turn is defined as an "oral conversation," 720 ILCS 5/14-1(b), (d), and there are no oral conversations at issue. [20] at 21 n.5. Defendants misread the statute. The IEA expansively defines an "eavesdropper" to include "any person . . . who acts as a principal," as Plaintiff has alleged here, and that person need not participate in a private (oral) conversation. 720 ILCS 5/14-1(b). Second, Defendant argues the text of the statute does not support holding a party to electronic communications liable for third-parties' interception of the communications. [27] at 14–15. But Defendant cites no legal authority for this position and the Court is not aware of any. To the contrary, at least one court has allowed a claim to proceed past the pleading stage on similar facts. *Kurowski I*, 683 F. Supp. 3d at 853. Finally, Defendant claims Plaintiff failed to identify any specific communications or circumstances indicating Plaintiff "intend[ed] the electronic communication to be private under circumstances reasonably justifying that expectation." [27] at 15 (discussing 720 ILCS 5/14-1(e)). Because Defendant raised

this argument for the first time in its reply brief, it is waived. *White v. United States*, 8 F.4th 547, 552 (7th Cir. 2021).

ii. Actual Damages

Finally, Defendant contends the Illinois Eavesdropping Act claim also fails because the Act only applies if a plaintiff alleges "actual damages" and, according to Defendant, Plaintiff has not alleged actual damages. [20] at 21–22. Plaintiff responds that she properly seeks actual damages, injunctive relief, and punitive damages under the IEA, and in any event, she has sufficiently stated a claim for actual damages at this stage of the litigation. [23] at 24–25.

The IEA permits the following remedies, among others, for violations of the Act: (a) an injunction to prohibit further eavesdropping; (b) actual damages against the eavesdropper or his principal or both; and (c) any punitive damages which may be awarded by the court or by a jury. 720 ILCS 5/14-6. As an initial matter, the IEA does not expressly require that a plaintiff show "actual damage" to seek recovery. This is a departure from the express language of other statutes that require a plaintiff must show actual damages. *Kurowski v. Rush Sys. for Health*, 2024 WL 3455020, at *8 (N.D. Ill. July 18, 2024) ("*Kurowski II*") (contrasting 720 ILCS 5/14-6(1) with 815 ILCS 505/10a(a) ("Any person *who suffers actual damage* as a result of a violation of [the Illinois Consumer Fraud and Deceptive Business Practices Act] committed by any other person may bring an action against such person.") (emphasis added)). Instead, the Act states that "*[a]ny or all* parties to any conversation or electronic communication upon which eavesdropping is practiced contrary to this Article shall

be entitled" to the Act's civil remedies, including injunctive relief and punitive damages. 720 ILCS 5/14-6(1) (emphasis added). Regardless, Plaintiff alleges she has suffered actual damages, which is sufficient on a motion to dismiss. [1] ¶ 140.

Defendant relies on *McDonald's v. Levine*, 439 N.E.2d 475 (Ill. App. Ct. 1982) for the proposition that "a plaintiff must prove he is entitled to damages in the same manner as he would in any common law tort action." [20] at 21 (quoting *McDonald's*, 439 N.E.2d at 480). Plaintiff does not contest this unremarkable statement of law and admits she must prove up actual and punitive damages at a later stage of litigation. [23] at 25.

Accordingly, the Court declines, in part, to dismiss Count III for violations of Section 5/14-2(a)(3) of the Illinois Eavesdropping Act. Plaintiff's claims that Defendant directed third-parties to illegally use an eavesdropping device on its behalf are dismissed.

IV. Conclusion

For the stated reasons, Defendant University of Phoenix's Motion to Dismiss [19], [20] is granted in part and denied in part. To the extent Plaintiff's VPPA claims are predicated on disclosures to Google, LinkedIn, TikTok, Microsoft, and Amazon, those claims are dismissed. Counts II and III may proceed as to disclosures to Facebook, Google, LinkedIn, TikTok, Microsoft, and Amazon.

E N T E R:

Dated: January 13, 2026

MARY M. ROWLAND
United States District Judge