UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

| | |
|---|---|
| AUSTIN ROTH, BRANDON ROSE, and ALEXANDER FONSECA, individually and on behalf of all others similarly situated,<br><br>Plaintiffs,<br><br>v.<br><br>WOOT.COM LLC, as a wholly owned subsidiary of AMAZON.COM SERVICES LLC,<br><br>Defendant. | CASE NO.<br><br>**CLASS ACTION COMPLAINT**<br><br>**JURY TRIAL DEMANDED** |

Plaintiffs Austin Roth, Brandon Rose, and Alexander Fonseca ("Plaintiffs"), individually and on behalf of all others similarly situated, by and through their undersigned counsel, bring this class action complaint against Defendant Woot.com LLC, as a wholly owned subsidiary of Amazon.com Services LLC ("Woot" or "Defendant"), which is engaged in the business of, among other things, the sale and delivery of pre-recorded audio-visual materials, including video games containing prerecorded content, through its website https://www.woot.com/ (the "Website"). Plaintiffs allege the following upon information and belief based on the investigation



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

of counsel, except as to those allegations that specifically pertain to Plaintiffs, which are alleged upon personal knowledge.

## NATURE OF THE ACTION

1. In recent years, courts across the country have recognized that opaque digital-information tracking practices pose a profound threat to Americans' privacy. The unauthorized collection of a person's browsing activity, website interactions, and device identifiers, particularly when the aforementioned information is combined with persistent identifiers that can link otherwise anonymous online activity to a specific individual, constitutes an unlawful invasion of the reasonable expectation of privacy that the federal Video Privacy Protection Act, the federal Wiretap Act, and analog state laws were enacted to protect.

2. Woot describes itself as the "original deals site" and claims that it offers "multiple daily deals and other short-term sales across seven (7) different categories."[1] Among the categories of products Woot sells and delivers through the Website are pre-recorded audio-visual materials, including video games that contain prerecorded video content. Website users can browse and purchase items directly from the Website, often at discount prices (the "Users"). Users can also acquire and/or purchase pre-recorded audio-visual materials through the Website, such as video games containing cut scenes ("Purchasers").

3. Users can sign in to the Website through a Woot or Amazon account. However, an Amazon account is required to purchase any item on the Website.[2]

4. Defendant begins placing and transmitting third-party tracking technologies immediately upon a User's initial visit to the Website, before Users receive any meaningful notice or opportunity to control the interception or dissemination of their data. Woot transmits Users' electronic communications and online activity to third-party advertising and analytics companies (the "Tracking Entities"), including Meta Platforms, Inc. ("Meta") (formerly known

[1] *Woot! FAQ,* WOOT, https://www.woot.com/faq?ref=w_ft_bs_rp&tab=general (last visited Mar. 16, 2026).
[2] *Changes to Woot!'s Payment Process*, WOOT (July 25, 2023) https://forums.woot.com/t/changes-to-woot-s-payment-process/1443009 (last visited Mar. 16, 2026).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

as Facebook, Inc.), through cookies, pixels, and similar tracking tools (the "Tracking Tools"). This tracking captures detailed interaction and behavioral data, including detailed URLs visited by Users, the name of products purchased by Users, the titles of buttons clicked by Users, forms filled out by Users, at what stage of the visit the User is in (e.g., product view, adding to cart, checking out, etc.), and other on-page elements interacted with by Users.

5. The data intercepted and collected by the Tracking Tools also includes routing and addressing information, including location information, IP addresses, and persistent identifiers used to identify the source of communications and the destination for the data. The Tracking Tools also capture and transmit device and technical identifiers such as device type, operating system, browser type, user identifiers that enable recognition across sessions and websites, and approximate geolocation data. The Tracking Entities use this data to infer Users' interests, preferences, age, location, or other characteristics based on the Users' behavior on the Website. Collectively, the information intercepted, collected, captured, and transmitted by the Tracking Tools to the Tracking Entities is referred to herein as "Sensitive Information."

6. Defendant does not disclose on the Website that Users' Sensitive Information would be captured by Tracking Tools on the Website, and then transmitted to the Tracking Entities, including Meta, for use in marketing and analytics activities conducted by the Tracking Entities and Defendant.

7. The Website's use of the Tracking Tools resulted in violations of the federal Video Privacy Protection Act (VPPA), 18 U.S.C. § 2710, and the federal Wiretap Act ("Wiretap Act"), 18 U.S.C. § 2510, et seq., as well as violations of analogous state wiretap statutes, and unlawful invasions into Users' privacy.

8. The Tracking Tools' capture and transmission of Users' Sensitive Information to the Tracking Entities is achieved through Defendant's knowing utilization of the Tracking Tools on the Website.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

9. Defendant chose to implement the Tracking Tools on the Website, the use of which allowed the Tracking Tools to transmit Users' Sensitive Information to the Tracking Entities, which includes data that identifies Users' requests and Purchasers' acquisition of video games containing cut scenes by title and description.

10. Included within the Sensitive Information exposed by Defendant's use of the Tracking Tools is information identifying Purchasers' acquisitions or requests for video games containing cut scenes, referred to herein as "Personal Video Information,"[3] which consists of Plaintiffs' and Purchasers' (i) Facebook ID ("FID," discussed and defined herein) and (ii) the detailed journey of Plaintiffs and Purchasers on the Website, showing their viewing and eventual purchase of pre-recorded audio video content in the form of video games containing cut scenes on the Website, including a detailed URL containing the name of that item and metadata containing an internal Content ID for that video game.[4]

11. At no point during or after the sign-up process, or anywhere on the Website for that matter, does Defendant seek or obtain adequate consent for the sharing of Users' Sensitive Information (which includes the subset of Purchasers' Personal Video Information), which was surreptitiously captured and transmitted through the Website's use of the Tracking Tools.

12. Defendant purposefully implemented and utilized the Tracking Tools to secretly facilitate the interception of Users' electronic communications[5] with the Website, in the form of their Sensitive Information. Defendant knew that the Tracking Tools would feed Users' communications to the Tracking Entities.

13. The Website does not provide notice of or obtain consent as to such practices.

---

[3] As used and defined herein, "Personal Video Information" is a subcategory of the defined term "Sensitive Information."

[4] *See* 18 U.S.C. § 2710(a)(3) (defining personally identifiable information under the VPPA as information able to identify users, as well as the title, description, or summary of video materials or services requested or obtained from a video tape service provider).

[5] The Wiretap Act defines "electronic communication" as any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system that affects interstate or foreign commerce. 18 U.S. C. § 2510(12).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

14. Users of the Website have been harmed by Defendant, resulting in violations of the federal Wiretap Act, the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 630, et seq., and the Florida Security of Communications Act ("FSCA"), Fla. Stat. § 934.01, et seq. In addition to monetary damages, Plaintiffs seek injunctive relief requiring Defendant to immediately (i) remove the Tracking Tools from the Website, or (ii) add, and obtain, appropriate consent from Users.

15. Plaintiffs' claims are brought as a class action, pursuant to Federal Rule of Civil Procedure 23, on behalf of themselves and all others similarly situated. Plaintiffs seek relief in this action individually and on behalf of Users of the Website for violations of the federal VPPA, 18 U.S.C. § 2710; the federal Wiretap Act, 18 U.S.C. § 2510, et seq.; CIPA, including Cal. Penal Code §§ 631 (illegal wiretapping) and 638.51 (unlawful use of a pen register or trap and trace device); California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, et seq.; the California Constitution at Art. 1, § 1; the FSCA, Fla. Stat. § 934.01, et seq., and common law.

## PARTIES

16. Plaintiff Austin Roth is and at all relevant times has been a citizen of California. Plaintiff Roth purchased pre-recorded audio-visual materials from the Woot Website in or around January 2026. On January 3, 2026, Plaintiff Roth purchased "Pokemon Scarlet" from the Website. Pokemon Scarlet is a video game that contains prerecorded video content in the form of animated cut scenes. Plaintiff Roth had previously purchased the video game "Tales of Graces f Remastered" from the Website. Plaintiff Roth visited the Website through a Firefox browser while logged into his Facebook account. Plaintiff Roth's Facebook profile includes his real name, location information (current and prior states of residency), personal photos, and other personal information that identifies Plaintiff Roth as a specific individual. At no point before, during, or after Plaintiff Roth's purchases did Woot request or obtain Plaintiff Roth's prior, informed, written consent (separate and distinct from any other legal or financial



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

obligations) to the disclosure of his Personal Video Information or other Sensitive Information to Meta or any other Tracking Entity. Following his interactions with the Website, Plaintiff Roth has observed Woot advertisements on social media platforms, including Instagram, and has experienced an apparent increase in video game-related advertisements from Woot in particular.

17. Plaintiff Brandon Rose is and at all relevant times has been a citizen of California. Plaintiff Rose purchased pre-recorded audio-visual materials from the Woot Website in or around March 2026. On March 5, 2026, Plaintiff Rose purchased "Metroid Prime 4 Beyond" from the Website. Metroid Prime 4 Beyond is a video game that contains prerecorded video content in the form of animated cut scenes. Plaintiff Rose had previously purchased the video game "Donkey Kong Country Returns HD." Plaintiff Rose visited the Website through a Firefox browser while logged into his Facebook account. Plaintiff Rose's Facebook profile includes his real name, location information (state of residency), personal photos, and other personal information that identifies Plaintiff Rose as a specific individual. At no point before, during, or after Plaintiff Rose's purchases did Woot request or obtain Plaintiff Rose's prior, informed, written consent (separate and distinct from any other legal or financial obligations) to the disclosure of his Personal Video Information or other Sensitive Information to Meta or any other Tracking Entity. Following his interactions with the Website, Plaintiff Rose has observed Woot advertisements on social media platforms, including Twitter and Instagram, and has experienced an apparent increase in video game-related advertisements from Woot in particular.

18. Plaintiff Alexander Fonseca is and at all relevant times has been a citizen of Florida. Plaintiff Fonseca purchased pre-recorded audio-visual materials from the Woot Website in or around February 2026. On February 26, 2026, Plaintiff Fonseca purchased "Dragon Ball: Sparking! Zero" for the Xbox Series X from the Website. Dragon Ball: Sparking! Zero is a video game that contains prerecorded video content in the form of animated cut scenes. Plaintiff Fonseca visited the Website through a Chrome browser while logged into his Facebook account. Plaintiff Fonseca's Facebook profile includes his real name, location information (current and



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

prior states of residency), educational history (including current school of attendance), personal photos, and other personal information that identifies Plaintiff Fonseca as a specific individual. At no point before, during, or after Plaintiff Fonseca's purchases did Woot request or obtain Plaintiff Fonseca's prior, informed, written consent (separate and distinct from any other legal or financial obligations) to the disclosure of his Personal Video Information or other Sensitive Information to Meta or any other Tracking Entity. Following his interactions with the Website, Plaintiff Fonseca has observed Woot advertisements on social media platforms, including Instagram, and has experienced an apparent increase in video game-related advertisements from Woot in particular.

19. Defendant Woot.com LLC is a subsidiary of Amazon.com Services LLC.[6] Woot owns and operates the Website, having its headquarters in Carrollton, Texas. Woot, through the Website, provides discounted access to a wide range of consumer products, including electronics, video games, household goods, apparel, and other merchandise, including product descriptions, specifications, pricing information, promotional materials, and detailed information regarding available products and related services.

## JURISDICTION AND VENUE

20. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1331 because it arises under the federal Wiretap Act, 18 U.S.C. § 2510, et seq., and the federal VPPA, 18 U.S.C. § 2710. This Court has supplemental jurisdiction over the non-federal claims in this action. This Court also has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members is more than 100, and at least one member of the Class defined below is a citizen of a different state that is diverse from Defendant's citizenship. Thus, minimal diversity exists under 28 U.S.C. § 1332 (d)(2)(A).

[6] *Who the HECK is Woot!,* WOOT, https://www.woot.com/about?ref=w_ngf_abt (last visited Apr. 21, 2026).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

21. This Court has personal jurisdiction over Defendant because Defendant has expressly consented to jurisdiction in this forum through its Terms of Use, which designate the state and federal courts located in King County, Washington, as the exclusive forum for disputes arising from use of its services. Defendant also maintains substantial business operations in this District and derives revenue from the operation and management of the Website, including through advertising, retail partnerships, and related commercial activity.

22. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant expressly designated the state and federal courts in King County, Washington, as the exclusive forum for disputes relating to the use of Woot's services via Woot's Terms of Use. Venue is also proper because Defendant conducts substantial business in this District, including through its management and operation of the Website and the commercial activities arising therefrom.

## FACTUAL ALLEGATIONS

### I. Legislative Background

#### A. The Video Privacy Protection Act

23. Congress enacted the VPPA in 1988 in response to a Washington, D.C. newspaper's profile of then-Supreme Court nominee Judge Robert H. Bork during his confirmation hearings. *See* S. Rep. No. 100–599, 2d Sess., at 5 (1988). The profile contained a list of 146 films Judge Bork and his family rented from a video store, obtained without his knowledge or consent. *Id.* Members of Congress denounced the disclosure as repugnant to the right of privacy. *Id.* at 5-8.

24. Congress passed the VPPA so that individuals can "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 (1988).

25. Senator Patrick Leahy explained that the new law was meant to protect "our right to privacy [in] the choice of movies that we watch with our family in our own homes," as



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

"[t]hese activities are at the core of any definition of personhood." 134 Cong. Rec. S5397–01, S. 2361 (May 10, 1988).

26. In 2012, Congress amended the VPPA "to reflect the realities of the 21st century." 158 Cong. Rec. H6849–01 (Dec. 18, 2012).

27. In a Senate Judiciary Committee meeting, Senator Leahy stated, "While it is true that technology has changed over the years, we must stay faithful to our fundamental right to privacy and freedom. Today, social networking, video streaming, the 'cloud,' mobile apps, and other new technologies have revolutionized the availability of Americans' information."[7]

28. Senator and Subcommittee Chair Hon. Al Franken stated:

> One way we need to update this law is to make sure that it is keeping up with technology. It used to be that if you wanted to watch a video, you had to go to the video store or then wait for it in the mail after that. Now you can stream it directly to your computer in seconds. Streaming is the future of video, . . . it is clear that the law does cover new technologies like streaming because it does not just cover ''prerecorded video cassette tapes.'' It also covers ''similar audio-visual materials.[8]

29. Courts across the country have affirmed a broad reading of the VPPA and its application to modern video sources, such as websites and video games.[9]

30. The VPPA protects consumers' information by prohibiting the disclosure of "personally identifiable information"[10] (PII), including information that would readily permit

---

[7] See *Committee on the Judiciary, Subcommittee on Privacy, Technology and the Law, The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century*, SENATE JUDICIARY COMMITTEE SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW, https://www.judiciary.senate.gov/download/hearing-transcript_-the-video-privacy-protection-act-protecting-viewer-privacy-in-the-21st-century (last visited Mar. 19, 2026).

[8] *Id.*

[9] See*, e.g., Mata v. Zillow Grp., Inc.*, No.: 24-cv-01095-DMS-VET, 2024 U.S. Dist. LEXIS 229061, at *8-9 (S.D. Cal. Dec. 18, 2024) (VPPA applied to real estate marketplace website); *Fan v. NBA Properties, Inc.*, No. 23-cv-05069-SI, 2024 U.S. Dist. 57205, at *3 (N.D. Cal. Mar. 26, 2024) (holding NFT digital platform is a VTSP subject to the VPPA); *Aldana v. GameStop, Inc.*, No. 22-CV-7063-LTS, 2024 U.S. Dist. LEXIS 29496, at *3 (S.D.N.Y. Feb. 21, 2024) (holding video game seller is a VTSP); *Sellers v. Bleacher Report, Inc.,* No. 23-cv-00368-SI, 2023 U.S. Dist. LEXIS 131579, at *15-18 (N.D. Cal. July 28, 2023) (VPPA sufficiently applied to sports news website); *Jackson v. Fandom, Inc.,* No. 22-cv-04423-JST, 2023 U.S. Dist. LEXIS 125531, at *6 (N.D. Cal. July 20, 2023) (VPPA applies to gaming and entertainment website); *Louth v. NFL*, No. 1:21-cv-00405-MSM-PAS, 2022 U.S. Dist. LEXIS 163706, at *11-12 (D.R.I. Sep. 12, 2022) (holding VPPA applied to NFL's videos accessible through mobile app).

[10] See 18 U.S.C. § 2710(a)(3).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

an ordinary person to identify a specific individual's video-watching behavior—here, Purchasers' Personal Video Information.

31. Congress made clear that the harm to individuals impacted by VPPA violations occurs the moment, and each time, a Purchaser's Personal Video Information is shared.

32. The VPPA requires that any consent to protected disclosures must be in a form that is "separate and distinct" from other legal and financial obligations, that such consent be informed and written, and that such consent be given prior to any disclosures. See 18 U.S.C. § 2710(b)(2)(B)(i)-(ii).

33. The VPPA covers "prerecorded video cassette tapes or similar audio visual materials,"[11] and Congress intended that to include a broad category of audio-visual materials, including "laser discs, open-reel movies, or CDI technology," digitally streamed "video clips," and video game cut scenes. See *Aldana,* 2024 U.S. Dist. LEXIS 29496, at *17-18, 19.

**1. Video Games as Audio-Visual Materials**

34. Video games contain "cut scenes"[12] and are designed to "keep players immersed in the game world by allowing them to follow a clear narrative."[13] A cut scene is a pre-recorded, non-interactive audio-visual sequence embedded within a video game.

35. "Narrative storytelling has become more and more common in video games . . . [and] [u]sing cinematic techniques and principles has helped game developers enhance gameplay experience for these kinds of games."[14]

36. As early as 1981, laser discs "permit[ted] the viewer to not only manipulate the programming, but to interact with the material – play games, take quizzes, adjust pacing and

[11] See 18 U.S.C. § 2710(a)(4).
[12] Cut scenes, also called cinematics, full motion videos, or interactive events, exist in several formats, including live action video, pre-rendered cut scenes, and real-time cut scenes. Each method makes use of pre-scripted events, and audio and video materials stored within a game's files. See David 'Ryatta' Wyatt, *The Art of Cutscenes*, INMOTION GAMING, http://www.inmotiongaming.com/the-art-of-cutscenes/ (last visited Mar. 18, 2026).
[13] *Game Development Meets Filmmaking: Cinematography in Video Games*, ACAD. OF ART UNIV. BLOG (Feb. 21 2020), https://blog.academyart.edu/game-development-meets-filmmaking-cinematography-in-video-games/ (last visited Mar. 18, 2026).
[14] *Id.*



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

repeat sections as desired."[15] VHS tapes could also contain interactive content, like the television series "Captain Power and the Soldiers of the Future," which used "video game technology" to create an interactive experience, emitting "a signal, encoded in the television film, that both activates and responds to light rays emitted by the toy – a jet aircraft with a pistol grip – when the user pulls the trigger."[16]

37. By the mid-1980s, Philips and Sony announced the development of a new video game medium based on the CD and CD-ROM technology.[17] This new format, called Compact-Disc Interactive, or CD-I, was developed to store larger volumes of combined audio, video, and computer graphics on a compact disc.[18]

38. By 1991, Philips introduced the Philips CDI 910, which "play[ed] cinema-quality computer games, educational programs, movies, and other multimedia products that combine video, audio, and text features in an interactive rather than a play-only mode."[19] The Philips CDI 910 played games like "Voyeur," for example, which was "a kind of high-tech version of Clue," allowing Users to "make decisions for characters and even change the outcome of the mystery."[20]

39. Sony unveiled its own console, the "PlayStation," which used a CD-ROM drive to "play videogames as well as other forms of interactive entertainment, as was considered important at the time."[21]

---

[15] Myron Berger, *High-Tech Equipment Comes of Age*, N.Y. TIMES, Sept. 27, 1981.
[16] Sandra Salmans, *The Interactive World of Toys and Television*, N.Y. TIMES, Oct. 4, 1987.
[17] See *Videodiscs in Healthcare: A Guide to the Industry*, THE MEDICALDISC REPORTER (1990), archived at https://tinyurl.com/44ypcaht (last visited Mar. 18, 2026).
[18] *See* ENCYCLOPEDIA OF LIBRARY AND INFORMATION SCIENCE VOL 50, SUPPLEMENT 13 (1992), archived at (last visited Mar. 18, 2026).
[19] Patrick Oster, *Philips's Multimedia Makeover; Dutch Electronics Firm Escapes Crisis, but Can It Compete Globally?*, WASH. PO. (Oct. 26, 1994) archived at https://tinyurl.com/4xwnausj (last visited March 18, 2026).
[20] David Elrich, *Interactive Video: Armchair Activities*, N.Y. TIMES (Dec. 9, 1993) archived at https://nyti.ms/3Wp2wkZ (last visited Mar. 18, 2026).
[21] IGN Staff, *History of the PlayStation: The greatest story ever told*, IGN (updated June 21, 2012 3:22pm EDT), archived at *https://tinyurl.com/25245e9t* (last visited Mar. 18, 2026).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

40. These technologies blurred the line between video games and movies, as "more and more movies look and sound like video games, and . . . more and more video games look and sound like movies . . . ."[22]

41. The advancement of these technologies has also opened the door for actors to take a greater part in a video game's narrative, with game developers using performance capture technology to record and translate actors' movements and facial expressions,[23] in addition to traditional acting performances.[24]

42. In the episode "How Cinematic Cutscenes in Video Games are Made" of "A Game Development Podcast," which is produced by Massive Entertainment, Cinematic Animator Soo Kang notes the basic purpose of a cinematic animator is "responsible for making the visual story telling of the game exciting, inspirational, fun, engaging, making sure that what you're seeing, on screen, the story telling, helps you progress with your gameplay as well . . . but just in general just fun to watch while you're sitting and taking a little break from gameplay . . . ."[25]

43. Soo Kang highlights the similarities between modern game cinematic production and film animation production: "[I]t just happened that I got my job in gaming industry first, but it wasn't too far off from what I learned about film animation because it was cinematic animation, . . . as opposed to game play animation for example . . . so they were not too far off."[26]

---

[22] Vincent Canby, *Are Video Games About to Zap the Action Movie?*, N.Y. TIMES (May 15, 1983) archived at https://tinyurl.com/5fv5s6v3 (last visited Mar. 18, 2026).

[23] *See* Anton Söderhäll, *Tracing the past, present, and future of game cinematics*, GAMES INDUSTRY (Jan. 25, 2022) https://www.gamesindustry.biz/tracing-the-past-present-and-future-of-game-cinematics (last visited Mar. 18, 2026).

[24] *See* Adam Sutton, *Videogame Voice Acting: So Bad, It's Good*, IGN (June 14, 2012 1:29 PM EDT) https://www.ign.com/articles/2011/03/04/videogame-voice-acting-so-bad-its-good (last visited Mar. 18, 2026; Jesse Schedeen, *Cyberpunk 2077, Keanu Reeves and 12 Other Movie Stars Who Made the Jump to Video* Games, IGN (Jan. 14, 2020 1:25 AM EDT) https://www.ign.com/articles/2019/06/11/cyberpunk-2077-keanu-reeves-and-12-other-movie-stars-who-made-the-jump-to-video-games (last visited Mar. 18, 2026).

[25] Massive Entertainment – A Ubisoft Studio, *How Cinematic Cutscenes in Video Games are Made | A Game Development Podcast*, YOUTUBE (Nov. 23, 2022), https://www.youtube.com/watch?v=WVQgeCZLjek (starting at 1:34) (last visited Mar. 18, 2026).

[26] *Id.* (starting at 6:22).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

44. Soo Kang went on to note that the difference between film and cinematic animation was not big because she was "applying the same learnings of the cinematic scene in the film, just in the game . . . maybe the transition is different . . . but, like, it wasn't, it didn't feel like I was starting from or reset from zero[.]"[27]

45. These advancements in game production were enabled by the technical advancements in the mediums used to store video games. Today, video games are typically manufactured using 100GB Blu-ray discs, the same audio-visual material used for movies.[28] Video games are also made available for download, with similar file sizes.[29]

**B. The Federal Wiretap Act**

46. The Wiretap Act, as amended through the 1986 Electronic Communications Privacy Act ("ECPA"), provides a private right of action for private intrusions as though they were government intrusions.[30]

47. In passing the ECPA, Congress was concerned about technological advancements, such as "large-scale mail operations, computer-to-computer data transmissions, cellular and cordless telephones, paging devices, and video teleconferencing."[31]

48. As a result, the ECPA primarily focused on two types of computer services, which were prominent in the 1980s: (i) electronic communications, such as email between users;

---

[27] *Id.* (starting at 6:55).

[28] Chaim Gartenberg, *Sony confirms PlayStation 5 name, holiday 2020 release data*, THE VERGE (Oct. 8, 2019) ("[T]he PS5 will use standard 100GB Blu-ray discs—Sony had previously confirmed that the console will offer a disc drive—but all games will have to be installed in the internal SSD this time around."), *available at* https://tinyurl.com/3z9spd9x (last visited March 18, 2026); *see also* Samuel Tolbert, *Can you use physical discs on PS5?*, ANDROID CENTRAL (Dec. 1, 2020) ("Cerny also confirmed that PS5 games are going to shop on 100GB Blu-ray discs."), *available at https://tinyurl.com/uchzpvt9* (last visited Mar. 18, 2026).

[29] As an example, Avatar: Frontiers of Pandora, a game from video game developer Ubisoft, requires a minimum of 90GBs of storage. *See Avatar: Frontiers of Pandora – Standard Edition*, UBISOFT, https://store.ubisoft.com/us/avatar--frontiers-of-pandora/60c30ca40d253c1914049e93.html?lang=en_US (last visited Mar. 18, 2026).

[30] Hayden Driscoll, *Wiretapping the Internet: Analyzing the Application of the Federal Wiretap Act's Party Exception Online*, 29 WASH. & LEE J. C.R. & SOC. JUST. 187, 192 (2022), https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=1541&context=crsj (last visited Mar. 19, 2026).

[31] Senate Rep. No. 99-541, at 2 (1986).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

and (ii) remote computing services, such as cloud storage or third-party processing of data and files.[32]

49. An ECPA claim requires a showing that a person or entity "(1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication, (5) using a device."[33]

50. "Interception" is defined as "aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

51. An "electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12).

52. The "paramount objective of the [ECPA] is to protect effectively the privacy of communications." *Joffe v. Google*, 746 F.3d 920, 931 (9th Cir. 2013).

53. The ECPA "protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers."[34]

54. Courts consistently hold that to violate the ECPA, an interception must be "contemporaneous" with the communication. *See, e.g., Fraser v. Nationwide Mutual Insurance Co.*, 352 F.3d 107, 113 (3d Cir. 2003); *Steve Jackson Games, Inc. v. Secret Service*, 36 F.3d 457, 460 (5th Cir. 1994); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 877-78 (9th Cir. 2002); *U.S. v. Steiger*, 318 F.3d 1039, 1047 (11th Cir. 2003).

[32] *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1103 (9th Cir. 2014).
[33] *R.C. v. Walgreen Co.*, 733 F. Supp. 3d 876, 900 (C.D. Ca. 2024) (quoting 18 U.S.C. § 2510, et seq.).
[34] *Bureau of Justice Assistance U.S. Department of Justice, Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510-2523*, BUREAU OF JUST., https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285 (last visited Mar. 19, 2025)



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

55. The "unauthorized duplication and forwarding of unknowing users' information" is among the most common methods of impermissible intrusion. *In re Facebook Inc. Internet Tracking Litig.*, 956 F.3d 589, 608 (9th Cir. 2020).

**C. The California Invasion of Privacy Act**

56. CIPA was enacted in 1967 for the expressly stated purpose "to protect the right of privacy of the people of [California]."[35] The California legislators were concerned about emergent technologies that allowed for the "eavesdropping upon private communications," believing such technologies "created a serious threat to the free exercise of personal liabilities and cannot be tolerated in a free and civilized society."[36]

57. CIPA is regularly recognized as California's analog to the Federal Wiretap Act, comprised of the same general elements and protect against the same general harms.

58. The California Legislature passed CIPA after finding and "declar[ing] that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Cal. Penal Code § 630.

59. To protect people's privacy, legislators broadly protected wired and aural communications being sent to or received from California.[37] Notably, for wired communications, California set out to prohibit (i) intentional wiretapping or (ii) willful attempts to learn the contents of wired communications, (iii) attempts to use or transmit information obtained through wiretapping, or (iv) aiding, agreeing with, employing, or conspiring with any person(s) to unlawfully do, permit, or cause the preceding three prongs.[38]

---

[35] Cal. Penal Code § 630.
[36] *Id.*
[37] Cal. Penal Code § 631-32.
[38] *Mastel v. Miniclip SA,* 549 F. Supp. 3d 1129, 1134 (E.D. Cal. 2021) (citing *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192 (1978)).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

60. CIPA attaches liability to any person who, willfully and without the consent of all parties to a communication, attempts to read or to learn the contents or meaning of any message or communication while it is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within California.[39]

61. CIPA looks to whether a user had a reasonable expectation of privacy, and courts analyzing the expectation of privacy look to the sensitivity of the data at issue. *See In re Facebook Inc. Internet Tracking Litig.*, 956 F.3d at 608. Legally protected or sensitive data have heightened requirements that demand more rigorous notice before intercepting.

62. CIPA also prohibits the installation of a "pen register" or a "trap and trace device" without first obtaining a court order.[40]

**D. The Florida Security of Communications Act**

63. Similar to the federal Wiretap and CIPA, the Florida Legislature passed the Florida Security of Communications Act ("FSCA"), Fla. Stat. § 934.01, et seq., after finding that "[i]n order to protect effectively the privacy of wire and oral communications, to protect the integrity of court and administrative proceedings, and to prevent the obstruction of intrastate commerce, it is necessary for the Legislature to . . . prohibit any unauthorized interception of such communications . . . ."[41]

64. The Florida Legislature further found that in order "[t]o safeguard the privacy of innocent persons, the interception of wire or oral communications when none of the parties to the communication has consented to the interception should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court."[42]

[39] Cal. Penal Code § 631(a).
[40] See Cal. Penal Code § 638.51.
[41] Fla. Stat. § 934.01(1).
[42] Fla. Stat. § 934.01(4).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

65. The FSCA "was modeled after [the federal Wiretap Act]" and "substantially follows the same language."[43] Notably, the Florida Supreme Court has held that the FSCA "evinces a greater concern for the protection of one's privacy interests" than the federal Wiretap Act and that it is "instructive to consult the legislative history of the federal act, as well as cases decided thereunder, for guidance on" interpreting the FSCA.[44]

66. Prior to 1974, "the [FSCA], like its federal counterpart, permitted the interception of defined wire or oral communications when one party to the communication gave consent.[45] However, the FSCA was amended in 1974 "to require *all parties* to a defined wire or oral communication to give prior consent."[46]

67. The 1974 amendment "was a policy decision by the Florida legislature to allow each party to a conversation to have an expectation of privacy from interception by another party to the conversation."[47]

68. Thus, "'[t]he [Florida] Legislature has determined as a matter of state public policy that the right of any caller to the privacy of his conversation is of greater societal value than the interest served by permitting eavesdropping or wiretapping.' Hence, the Florida act evinces a greater concern for the protection of one's privacy interests in a conversation than does the federal act."[48]

69. Further mirroring the development of its federal counterpart, two years after Congress amended the Wiretap Act via the 1986 enactment of the ECPA, "[t]he Florida legislature substantially revised chapter 934 in 1988 to conform with the federal provisions regarding the interception of wire, oral, or electronic communications."[49]

---

[43] *Mozo v. State*, 632 So. 2d 623, 629 (Fla. Dist. Ct. App. 1994).
[44] *Id.* (citing *State v. Tsavaris*, 394 So. 2d 418, 422 (Fla. 1981), rev'd on other grounds, *Dean v. State*, 478 So. 2d 38 (Fla. 1985)).
[45] *State v. Tsavaris*, 394 So. 2d at 422.
[46] *Id.* (emphasis in original).
[47] *Id.* (quoting *Shevin v. Sunbeam Television Corp.*, 351 So. 2d 723, 726-27 (Fla. 1977)).
[48] *Id.* (quoting *State v. Walls*, 356 So. 2d 294, 296 (Fla. 1978)) (internal citation omitted).
[49] *State v. Jackson*, 650 So. 2d 24, 27 (Fla. 1995).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

70. The Florida Legislature added electronic communications to chapter 934 of the FSCA to address the growing need for protection of unauthorized interception of electronic communications arising from the proliferation of digital communication devices such as cellular telephones and pagers.[50]

71. The purview of the FSCA's protection of electronic communications extends to emails, digital instant messages, and the like. Indeed, "[t]he clear intent of the Legislature in enacting section 934.03 was to make it illegal for a person to intercept wire, oral, or electronic communications" and "it is beyond doubt" that emails, digital chat conversations, and/or instant messages are electronic communications protected by the FSCA.[51]

**E. How Websites Function**

72. Websites are hosted on servers, in the sense that their files are stored on and accessed from servers. Websites are, in part, "run" on a user's internet browser, as the browser loads and processes the website's code to display the webpage.

73. Websites are a collection of webpages. A webpage is essentially a document containing text written in HyperText Markup Language (HTML) code.[52]

74. Each webpage has a unique address, and two webpages cannot be stored at the same address.[53]

75. When a user navigates to a webpage (by entering a URL address directly or clicking a hyperlink containing the address), that user's browser contacts the DNS (Domain Name System) server, which translates the web address of that website into a unique IP (Internet Protocol) address.[54]

---

[50] *Id.*
[51] *O'Brien v. O'Brien*, 899 So. 2d 1133, 1135-36 (2005).
[52] *What is the difference between webpage, website, web server, and search engine?*, MOZILLA, https://developer.mozilla.org/en-US/docs/Learn/Common_questions/Web_mechanics/Pages_sites_servers_and_search_engines (last visited Mar. 18, 2026).
[53] *Id.*
[54] *How the web works*, MOZILLA, https://developer.mozilla.org/en-US/docs/Learn/Getting_started_with_the_web/How_the_Web_works (last visited Mar. 18, 2026).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

76. An IP address is "a unique address that identifies a device on the Internet or a local network."[55] Essentially, an IP address is:

> The identifier that allows information to be sent between devices on a network: they contain location information and make devices accessible for communication. The internet needs a way to differentiate between different computers, routers, and websites. IP addresses provide a way of doing so and form an essential part of how the internet works.[56]

77. When a user's browser navigates to a webpage, it sends an HTTP request to the server identified by the webpage's IP address. This request is for the specific resource located at the URL. If the server fulfills this request, it issues an HTTP response, which includes the status of the request and, typically, the requested content. This content is then transmitted in small chunks, known as data packets, and reassembled into the complete webpage by the user's browser upon arrival.[57]

78. This Request URL includes a domain name and path, which identify the specific content being accessed on a website and its location within the website's structure.

79. The Request URL typically contains parameters. Parameters are values added to a URL to transmit data to the recipient, prefaced by a question mark to signal the use of parameters. Parameters direct a web server to provide additional context-sensitive services,[58] as depicted below:


*Figure 1 - Mozilla's diagram of a URL, including parameters*[59]

80. Website owners or web developers choose and manage the URLs for their websites.

---

[55] *What is an IP Address – Definition and Explanation*, KASPERSKY, https://usa.kaspersky.com/resource-center/definitions/what-is-an-ip-address (last visited Mar. 18, 2026).
[56] *Id.*
[57] *Id.*
[58] To see examples of how Defendant used parameters to provide additional information here, *see, infra,* Section C(2).
[59] *What is a URL?*, MOZILLA, https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_URL (last visited Mar. 18, 2026).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

81. URL encoding is an essential process to ensure that data is safely transmitted via URLs. URL encoding converts characters into a format that can be transmitted over the Internet.[60] For example, URLs cannot contain spaces; URL encoding normally replaces a space with a plus (+) sign or with %20.

82. The American Standard Code for Information Interchange (ASCII) was designed in the early 1960s as a standard character set for computers and electronic devices.[61] Today, UTF-8 is the Internet's most common character encoding.[62]

83. URL decoding is the process of URL encoding in reverse so that the URL is in a more readable format.[63] To demonstrate:

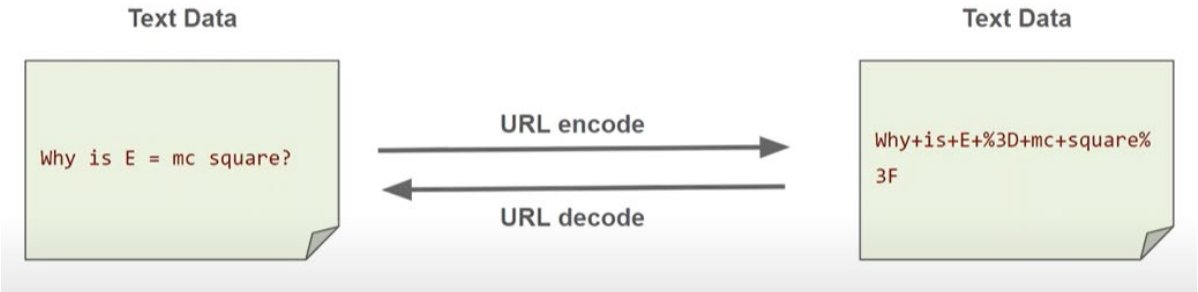



*Figure 2 – Demonstrating URL encoding and decoding*[64]

84. Similarly, parameters and metadata can be parsed and separated into easily reviewed, searchable formats.

85. After sending the Request URL, and after the server responds to the Request URL, the user's browser assembles the packets sent by the server back into the HTML code of the webpage, which is then processed by the user's browser, as it arrives,[65] and "rendered" into

---

[60] *Id.*

[61] *HTML ASCII Reference*, W3 SCHOOLS, https://www.w3schools.com/charsets/ref_html_ascii.asp (last visited Mar. 19, 2026).

[62] *UFT-8*, MOZILLA, https://developer.mozilla.org/en-US/docs/Glossary/UTF-8 (last visited Mar. 18, 2026).

[63] *What IS URL Decoding and URL Encoding?*, GOCHYU (Oct. 18, 2020), https://gochyu.com/blog/url-encode-decode (last visited Mar. 18, 2026).

[64] Viraj Shetty, *URL Encoding in a few minutes*, YOUTUBE (Sept. 5, 2023), https://www.youtube.com/watch?v=ru0iCHsmsLc (last visited Mar. 19, 2026).

[65] This processing of webpage data as it arrives is called "parsing," and allows web browsers to convert raw data received over the internet into structured data objects used by the renderer built-in to the browser to create images on the screen. This means that, unless a software command, like a Tracking Tool, is physically last to arrive at a device, it is loaded and executed before the communication has finished being received. See *Populating the page:*



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

a visual display according to the instructions of the HTML code.[66] This is the visible, and usually interactable, website that most people think of.

86. To provide more complex website functionalities, website developers will include more complex commands written in other computer programming languages, such as JavaScript snippets, within the HTML documents.[67]

87. Such complex tasks include streaming videos by Users or subscribing to Newsletters/ Digital/Print Magazine, or code used to monitor and report User activity.

88. In short, the Internet relies on a constant back-and-forth stream of requests and responses between a user's browser and a website's stored code and data. Importantly, the requests and responses provide a perfect snapshot of everything a user does (or does not do) on a website, and when and how they do it, and with what software and hardware.

89. Unbeknownst to Users, as they browse the Website, the Tracking Tools, including third- and first-party cookies, capture and record both incoming and outgoing requests and responses that make up their entire experience on the Website.

## II. Woot and the Meta Tracking Pixel

### A. The Meta Pixel as a Tracking Tool

90. Boasting 2.9 billion monthly active users, Facebook is the largest social networking site on the planet.[68] Facebook is a "real identity platform,"[69] meaning users are allowed only one account and must share "the name they go by in everyday life."[70] To meet that

---

*how browsers work*, MOZILLA, https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_URL (last visited Feb. 20, 2026).

[66] *What is a URL?*, MOZILLA, https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_URL (last visited Sept. 17, 2024).

[67] *See JavaScript Basics*, MOZILLA, https://developer.mozilla.org/en-US/docs/Learn/Getting_started_with_the_web/JavaScript_basics (last visited Nov. 18, 2024).

[68] 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 (last visited Mar. 19, 2026).

[69] Sam Schechner and Jeff Horwitz, *How Many Users Does Facebook Have? The Company Struggles to Figure It Out*, WALL. ST. J. (Oct. 21, 2021 4:05 PM ET). https://www.wsj.com/articles/how-many-users-does-facebook-have-the-company-struggles-to-figure-it-out-11634846701 (last visited Mar. 19, 2026).

[70] *Community Standards, Part IV Integrity and Authenticity*, FACEBOOK, https://www.facebook.com/communitystandards/integrity_authenticity (last visited Mar. 19, 2026).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

goal, Facebook requires users, when creating an account, to provide their first and last name, along with their birthday and gender.[71]

91. Approximately seven-in-ten U.S. citizens have a Facebook profile[72] – all of whom provided the same personal information to Meta when creating their Facebook profiles.

92. Facebook monetizes account holders by selling companies access to their Facebook feeds, including to website owners like Defendant.[73]

93. Facebook's advertising capabilities are valuable because of its ability to effectively target Users with meaningful or relevant advertising.[74] Facebook can target Users so effectively because it monitors and analyzes user activity both on and off its site.[75] This allows Facebook to infer details about Users beyond what Users explicitly disclose, like their "interests," "behavior," and "connections."[76] Facebook compiles this information into a generalized dataset called "Core Audiences," which website owners can sort through using highly specific filters and parameters to ensure their targeted advertisements reach Users likely to respond positively.[77]

94. Website owners can build "Custom Audiences,"[78] which enable them 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."[79] Meta's Custom Audience feature enables direct targeting of existing customers and the building of "Lookalike Audiences," which

---

[71] *Sign Up*, FACEBOOK, https://www.facebook.com/ (last visited Mar. 19, 2026).
[72] Katherine Schaeffer, *5 Facts about how Americans use Facebook, two decades after its launch*, PEW RSCH. CTR. (Feb. 2, 2024), https://www.pewresearch.org/short-reads/2024/02/02/5-facts-about-how-americans-use-facebook-two-decades-after-its-launch/ (last visited Mar. 19, 2026).
[73] 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. (last visited Mar. 18, 2026).
[74] *About Meta Pixel*, FACEBOOK, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Mar. 18, 2026).
[75] *Id.*
[76] *Audience ad targeting,* META, https://www.facebook.com/business/ads/ad-targeting (last visited Mar. 19, 2026).
[77] *Easier, More Effective Ways to Reach the Right People on Facebook*, FACEBOOK, https://www.facebook.com/business/news/Core-Audiences (last visited Mar. 19, 2026).
[78] *About custom audiences*, FACEBOOK, https://www.facebook.com/business/help/744354708981227?id=2469097953376494 (last visited Mar. 19, 2026).
[79] *About an events custom audience*, FACEBOOK, https://www.facebook.com/business/help/366151833804507?id=300360584271273 (last visited Mar. 19, 2026).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

"leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[80] Unlike Core Audiences, Custom Audiences require an advertiser to supply Users' data to Meta. Website owners can do so through two mechanisms: manually uploading customer contact information in the form of "lists," or using Meta's "Business Tools," which automatically collect and transmit the data.[81]

95. Here, Defendant made use of Meta's Business Tools and lists to disclose Users' Sensitive Information to Meta.

96. For example, Meta offers the Meta Pixel and the Conversions API ("CAPI"). Where "the Pixel lets you share web events from a web browser[,] . . . the Conversions API lets you share web events directly from your server."[82]

97. It is important to note that, with trained investigators, some Meta Pixel behavior is observable on a user's device; investigators and users have no method of determining whether websites make use of CAPI on websites' servers or what information is collected by the CAPI.

98. The Meta Pixel is a piece of code that website owners, like Defendant, can integrate into their websites. Once activated, the Meta Pixel "tracks the people and types of actions they take. . . ."[83] When the Meta Pixel captures an action, it sends a record of the action to Meta. After receiving the Pixel transmission sent by a website owner, Meta processes it, analyzes it, and assimilates it into datasets like the Core Audiences and Custom Audiences.

99. Because Meta designs the Meta Pixel to be installed onto Users' browsers, as well as the system receiving the information, it is in complete control of how simple or complex its transmissions appear. For example, Meta requires that website owners encode their Meta

---

[80] *About lookalike audiences*, FACEBOOK, https://www.facebook.com/business/help/164749007013531?id=401668390442328 (last visited Mar. 19, 2026).
[81] *Create a customer list custom audience*, FACEBOOK, https://www.facebook.com/business/help/170456843145568?id=2469097953376494 (last visited Mar. 19, 2026);.
[82] *Omni Optimal Technical Setup Guide: Best Practices and Requirements*, FACEBOOK, https://developers.facebook.com/documentation/ads-commerce/marketing-api/best-practices/omni-optimal-setup-guide (last visited Apr. 14, 2026).
[83] *Retargeting*, FACEBOOK, https://www.facebook.com/business/goals/retargeting (last visited Mar. 19, 2026).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Pixel transmissions using UTF-8, a process that prepares data for transmission across the Internet.

100. The Meta Pixel collects and sends all the information needed to identify in a single transmission, including IP addresses.[84] The Meta Pixel does not require obtaining any additional information from other websites to piece together Users' identities.

101. Meta's "Get Started" page further explains how it can identify Users and match them to their Facebook pages: "[The Meta Pixel] relies on Facebook cookies, which enable us to match your website visitors to their respective Facebook User accounts. Once matched, we can tally their actions in the Facebook Ads Manager so you can use the data to analyze your website's conversion flows and optimize your ad campaigns."[85]

102. Meta designed the Meta Pixel, as well as the computer system that receives and parses the data that the Meta Pixel intercepts, collects, and transmits to Meta. Meta had total control over the form, function, and complexity of the Request URLs generated through the Meta Pixel, and the data collected and transmitted by the Meta Pixel was as easy or as difficult to read as Meta desired.

103. Meta designed the information received via Meta Pixel transmissions so that any ordinary person can read and understand the contents of information shared with Meta.

104. Even though some of the information disclosed is technical in nature, any ordinary person can easily surmise what pre-recorded audio-visual materials a person requested or obtained because it directly tracks the name of the pre-recorded audio-visual materials as it appears on the User's screen, as well as that person's FID — an easily identifiable and unique string of numbers tied to the individual.

105. Indeed, Meta controlled how this information was transmitted and received. Meta chose to use the most common encoding system to transmit data across the Internet, an encoding

[84] *See Customer Information Parameters*, META, https://developers.facebook.com/docs/marketing-api/conversions-api/parameters/customer-information-parameters/ (last visited Mar. 19, 2026).
[85] *Get Started*, META, https://developers.facebook.com/docs/meta-pixel/get-started/ (last visited Mar. 18, 2026).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

system that common internet browsers can easily decode and parse into easy-to-understand information.

106. After receiving the Meta Pixel transmissions, Meta also leveraged the received data to build detailed profiles for targeted advertising based on a consumer's activities (including purchases), interests, webpage history, searched-for content, behavior, and habits.

107. After processing the Meta Pixel-collected data, Meta also makes much of the data available to the website owner through the "Event Manager" tool.[86]

108. However, to make use of the Meta Pixel, website operators and/or owners, such as Defendant, must first agree to the Meta Business Tools Terms.

109. The Meta Business Tools Terms directly inform website developers who implement the Meta Pixel of how it operates.

110. Meta explicitly informs website developers that implement the Meta Pixel that using the Meta Pixel will result in Meta receiving Users' information "that personally identifies [them] . . . " ("Contact Information") and information "about [Users] and the actions that they take on your websites . . ." ("Event Data").[87] The terms also warn website developers that Facebook will "process the Contact Information solely to match the Contact Information against" FIDs, "as well as to combine those [FIDs] with corresponding Event Data."[88]

111. Meta also requires website developers that implement the Meta Pixel to "represent and warrant that [they] . . . have all the necessary rights and permissions and a lawful basis (in compliance with all applicable laws, regulations and industry guidelines) for the disclosure and use of Business Tool Data."[89]

---

[86] *About Meta Events Manager*, FACEBOOK, https://www.facebook.com/business/help/898185560232180?id=1205376682832142 (last visited Mar. 18, 2026).

[87] *Meta Business Tools Terms, Section 1(a)(i)-(ii)*, FACEBOOK, https://www.facebook.com/legal/businesstech?paipv=0&eav=AfY4CZdRHnQNL2-VtXBCcMUcg-6J-5jU8AL4hOLViKhAWi-SbNmA4QuXlc6yyk877eY&_rdr (last visited Mar. 19, 2026).

[88] *Id.* § 2(a)(i)(1).

[89] *Id.* § 1(e).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

112. Additionally, Meta requires website developers that implement the Meta Pixel to "represent and warrant that [they] will not share Business Tool Data with [Meta] that . . . includes . . . categories of sensitive information (including any information defined as sensitive under applicable laws, regulations and applicable industry guidelines)." [90]

113. In short, Meta explicitly describes that the Meta Pixel combines users' identifying information with their activity on websites to build marketing profiles and, as a result, that websites should not share sensitive information using the Meta Pixel.

114. Despite Meta's warnings, website owners ultimately have control over what actions—or, as Meta calls it, "events"—the Meta Pixel will monitor on websites. These events, in turn, determine what data is collected, including the website's query string parameters, metadata, and what pages a visitor views.[91]

115. Defendant, as a website owner, can widen or narrow the scope of information transmitted or received by Users interacting with the Website and, as a result, captured by Meta. Defendant also has some ability to limit how Meta Pixel identifies Users through cookies.

116. While Defendant's Website has configured the Meta Pixel to automatically collect "HTTP Headers" and "Pixel-specific Data," Defendant chooses which events to monitor and which parameters and metadata are collected and sent to Meta.[92]

117. HTTP Headers include "IP addresses, information about the web browser, page location, document, referrer, and data potentially identifying persons using the website."[93] Pixel-specific Data includes "the Pixel ID and cookie[s],"[94] which can also identify persons using the website.

---

[90] *Id.* § 1(h).
[91] *See Meta Pixel, Accurate Event Tracking, Advanced*, FACEBOOK, https://developers.facebook.com/docs/facebook-pixel/advanced/ (last visited Mar. 19, 2026); *see also Best practices for Meta Pixel setup*, FACEBOOK, https://www.facebook.com/business/help/218844828315224?id=1205376682832142 (last visited Mar. 19, 2026).
[92] *Meta Pixel*, FACEBOOK, https://developers.facebook.com/docs/facebook-pixel/ (last visited Mar. 18, 2026).
[93] *Id.*
[94] *Id.*



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

118. Website owners can configure the Meta Pixel to track events other than Meta's menu of "standard events," which contain events that can track what content a visitor views or purchases.[95] A website owner can also create their own "custom events," allowing them to track designated user activity and data through events programmed specifically for that purpose on the advertiser's website.[96]

119. The Meta Pixel activates when one of the events being monitored by a website occurs, such as loading a web page or a specified action, such as clicking a button.

120. Once the Meta Pixel activates, it copies relevant information from the communication between the user and website, such as URLs, user activity, search terms, metadata, query string parameters, and Pixel-specific Data, including cookies. The Meta Pixel then bundles that information together and transmits that copied bundle to Meta through a "GET" or "POST" HTTP Request.

121. The Request URL generated by the Meta Pixel contains much of this information as parameters, while cookies are included in the HTTP Headers. *See Figure 13*.

**B. Woot Implemented the Meta Pixel on the Website.**

122. To activate and employ the Meta Pixel, a website owner must first sign up for a Facebook account, where adding the Meta Pixel to the website owner's "business portfolio" provides the most utility for using the Meta Pixel.[97] For instance, business portfolios can: (i) create and utilize more simultaneous Pixels, (ii) manage multiple Facebook Pages, Instagram accounts, ad accounts, and catalogs from a centralized interface, (iii) access and manage multiple parties (which can then be given specific levels of access, including more easily revoking access to ex-employees), (iv) post or analyze data analytics collected from Facebook

[95] *Specifications for Meta Pixel standard events*, FACEBOOK, https://www.facebook.com/business/help/402791146561655?id=1205376682832142 (last visited Mar. 19, 2026).
[96] *About standard and custom website events*, FACEBOOK, https://www.facebook.com/business/help/964258670337005?id=1205376682832142 (last visited Mar. 19, 2026).
[97] *How to set up your Meta Pixel with a business portfolio*, FACEBOOK, https://www.facebook.com/business/help/314143995668266?id=1205376682832142 (last visited Mar. 19, 2026).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

pages or Instagram accounts, (v) run ads businesses across Facebook and Instagram, and (vi) create and manage shops across Facebook and Instagram.[98]

123. To add an operational Meta Pixel to a website, the website owner or operator must take several affirmative steps, including naming the Meta Pixel during the creation and setup of the Meta Pixel.[99]

124. The website owner or operator must tell Meta which website events it wants to track, and Meta then returns the corresponding Meta Pixel code for the website owner or operator to incorporate into its website.

125. Moreover, Meta notes that "[d]evelopers and marketers can ***optionally choose*** to send additional information about the visit through Custom Data events."[100]

126. Specifically, Defendant chose to send to Meta the names of video games purchased on the Website that contain cut scenes, the URL of the purchased video game (which clearly identified the purchased video game by title and internal Content ID), and the Purchaser's FID. Defendant made a conscious decision to share Purchasers' Personal Video Information with Meta.

127. Once the Meta Pixel is installed, the website operator assigns access to the Meta Pixel to specific people for management purposes,[101] and must connect the Meta Pixel to a Facebook Ad account.[102]

128. After following these steps, a website operator can start capturing and sharing information using the Meta Pixel.

---

[98] *About business portfolios*, FACEBOOK, https://www.facebook.com/business/help/486932075688253 (last visited Mar. 19, 2026).

[99] *Id.*; *see also* Ivan Mana, *How to Set Up & Install the Facebook Pixel*, YOUTUBE (Feb. 4, 2022) https://www.youtube.com/watch?v=ynTNs5FAUm8 (last visited Mar. 19, 2026).

[100] *Meta Pixel*, META, https://developers.facebook.com/docs/meta-pixel/ (last visited Mar. 19, 2026) (emphasis added).

[101] *Add people to your Meta Pixel in Meta Business Suite or Business Manager*, FACEBOOK, https://www.facebook.com/business/help/279059996069252?id=2042840805783715 (last visited Mar. 19, 2026).

[102] *Add an ad account to a Meta Pixel in Meta Business Manager*, FACEBOOK, https://www.facebook.com/business/help/622772416185967 (last visited Mar. 19, 2026).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

129. To be clear, the Meta Pixel cannot be placed on a website solely by Meta. It must be placed directly by or on behalf of the site owner. Woot did just this.

### C. The Facebook ID Allows an Ordinary Person to Identify a Purchaser and Their Video Game Purchases

130. Meta maintains vast amounts of data on each of its account holders, like Plaintiffs and the putative Class Members.

131. In addition to the information every user is required to provide to Meta when creating an account (including first and last name, date of birth, gender, email address and/or phone number, and password), Meta also possesses and has access to all of the information every user has ever posted on his or her Facebook profile, profile views, likes, comments, shared and/or reposts, event invitations, event RSVPs, Facebook messages, "check-ins," and much, much more.

132. This data is not limited to only what a person does on Facebook but also includes all records relating to when a user is tracked on off-Facebook websites, such as Plaintiffs', Website Users', and Purchasers' interactions with the Website.

133. The Meta Pixel continuously adds data from new interactions to the historical profiles Meta maintains on individuals with Facebook profiles (and even for a time after Facebook account holders delete their Facebook profiles).

134. Crucial to the Meta Pixel's effectiveness is its ability to associate a user's interactions on websites across the internet with that specific user's unique Facebook profile. This is made possible, most notably, through the FID.

135. An FID—commonly known as the "c_user field—is a unique and persistent identifier that Facebook assigns to each user. It contains a series of numbers used to identify a specific profile, as depicted below:


*Figure 3 - Sample FID number of test account created by Plaintiffs' counsel in a prior investigation into the Meta Pixel, captured by a Meta Pixel event*



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

136. An FID can be used by anyone to easily identify a Facebook account holder by simply appending the FID to www.facebook.com (e.g., www.facebook.com/[FID_here]).

137. Meta itself publishes explanations and help center materials confirming that an FID is a string of numbers that links to a specific profile and can be entered into the URL bar to navigate directly to that profile. Ordinary internet users – roughly seven-in-ten Americans – are among Facebook's account holder base and regularly encounter URLs and learn from Facebook's own help pages on how to find and use FIDs.[103]

138. A simple search for "what is a c_user cookie" leads one to learn that the string of numbers is the FID of the user, demonstrating that even non-technical internet users can, without specialized knowledge, discover and apply an FID to locate a given Facebook profile.

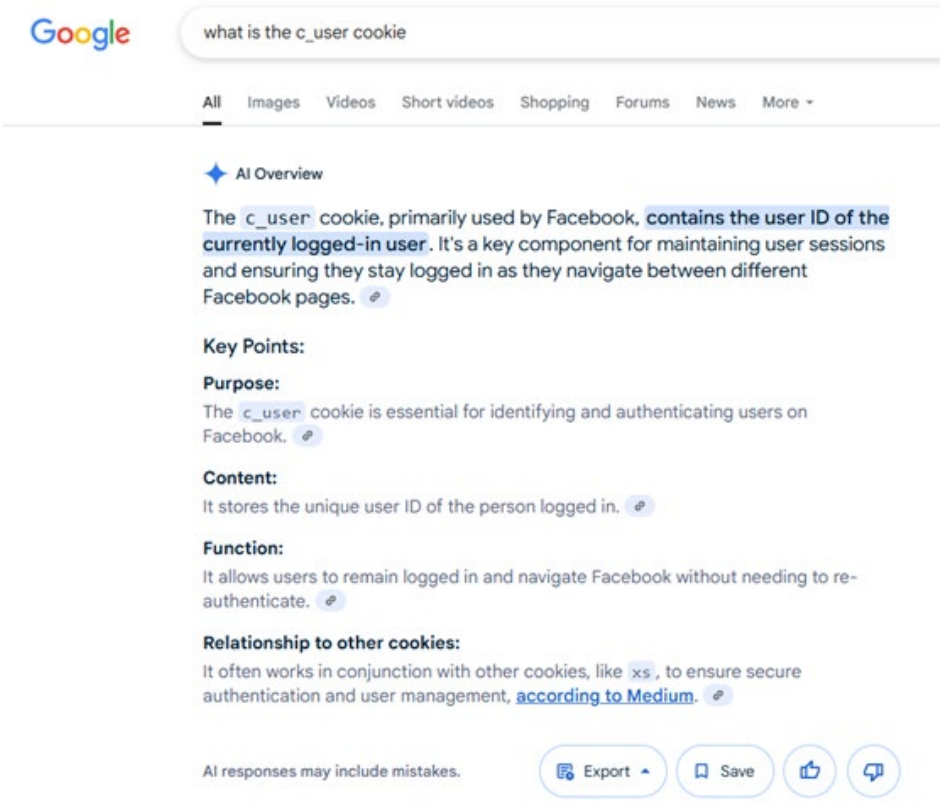



*Figure 4 – Google AI answer to search for "what is the c_user cookie"*

[103] Katherine Schaeffer, *5 Facts about how Americans use Facebook, two decades after its launch*, PEW RSCH. CTR. (Feb. 2, 2024), https://www.pewresearch.org/short-reads/2024/02/02/5-facts-about-how-americans-use-facebook-two-decades-after-its-launch/ (last visited Mar. 19, 2026).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

139. A subsequent Google search for "facebook user id" reveals that the URL of a Facebook profile is facebook.com followed by the FID.

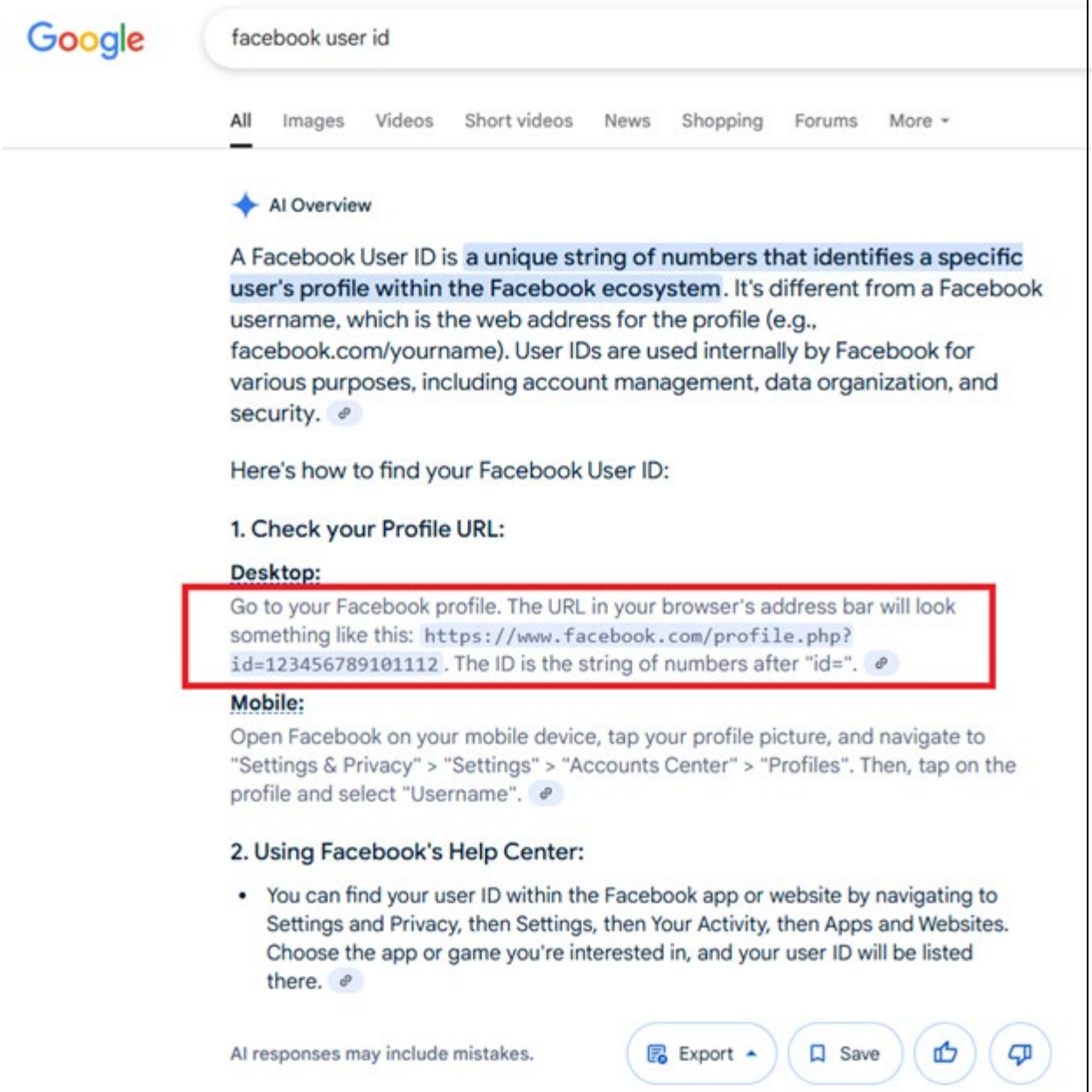



*Figure 5 – Google AI answer to search for "facebook user id"*

140. Even simpler, with the rise in general artificial intelligence agents such as ChatGPT, anyone with an internet connection can use tools to decipher computer code, as demonstrated below.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

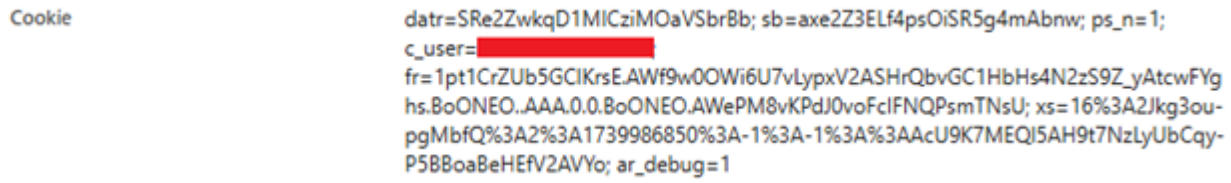



*Figure 6 – Screenshot from a browser's developer tools of cookies transmitted from a Pixel transmission (c_user redacted)*

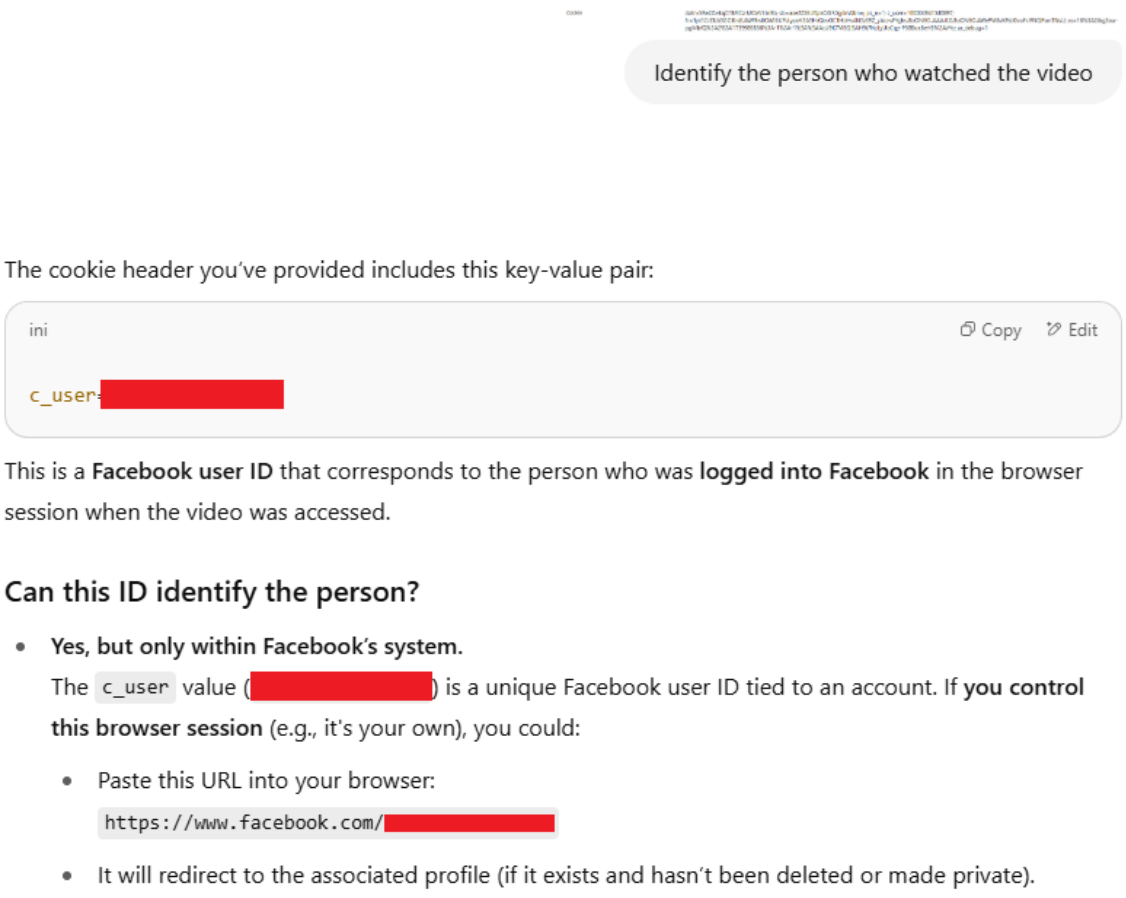



*Figure 7 – Screenshot from ChatGPT response to query "Identify the person who watched the video" with screenshot of cookies from Figure 18 (c_user redacted)*

141. To illustrate, appending the FID from *Figure 3* to the Facebook URL in a standard internet browser (here, www.facebook.com/100091959850832) will redirect the webpage straight to the Facebook profile associated with the FID, as depicted below:



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

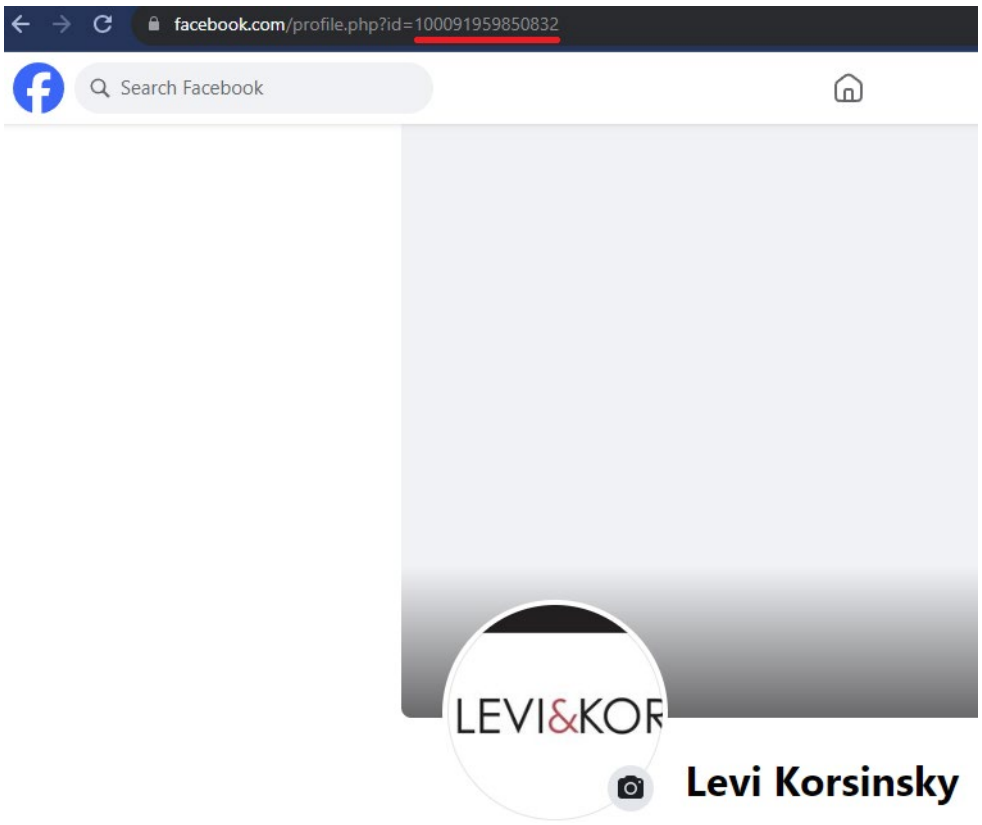



*Figure 8 - Sample result of appending FID of a user to "facebook.com/" being redirected to the user's profile created by Plaintiffs' counsel in a prior investigation into the Meta Pixel*

142. Thus, when a URL embedding an FID is disclosed – such as by a video tape service provider, any ordinary user who follows that link will be brought directly to the Facebook profile operating under that ID, thereby identifying the person who purchased the pre-recorded audio-visual material and revealing any public details displayed on that profile (e.g., photos, posts, Facebook friends, location, occupation, partner/spouse, educational history, etc.).

143. Importantly, some Facebook profile information – name, gender, profile photo, cover photo, username, user ID (account number), age range, language, and country – is "always public."[104] No privacy setting on a Facebook account would allow Plaintiffs, or any account holder, to hide this basic information.

[104] *Control who can see what you share on Facebook*, FACEBOOK, https://www.facebook.com/help/1297502253597210 (last visited Mar. 19, 2026).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

144. An FID identifies an individual with far greater precision than a name alone, particularly where the name is common or duplicated. For example, while multiple individuals named "John Smith" may exist in the United States—or even on Facebook—only one account will correspond to a particular FID. Possession of an FID, therefore, allows identification of a unique individual with certainty.

145. Even if a Facebook profile's displayed name is a pseudonym, the underlying FID still furnishes a clear hook by which Tracking Entities can associate specific viewing behavior with a single, uniquely identified human being.

146. Here, for each of Plaintiffs' interactions on the Website, the Meta Pixel transmitted those interactions to Meta, which was then able to instantly associate those interactions with Plaintiffs' Sensitive Information submitted when creating their accounts, and with any Sensitive Information ever available on their Facebook profiles through their unique FIDs.

147. Thus, an FID is not an obscure technical ingredient that needs to be combined with many other opaque identifiers, but instead a readily accessible identifier that ordinary people can understand and use to connect personal names, profiles, and online activities to the identifier.

**D. The Meta Pixel Employed by Woot Shared Users' Sensitive Information**

148. Defendant added the Meta Pixel to the Website, which it used to invisibly track Users throughout their use of the Website. The Meta Pixel tracks User activity on web pages by monitoring events[105] that, when triggered, cause the Meta Pixel to automatically send data, including Users' Sensitive Information, directly to Meta.[106] Examples of events utilized by websites include: (i) a user loading a page with a Pixel installed (the "PageView event");[107] (ii)

[105] *About Meta Pixel*, FACEBOOK, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Mar. 19, 2026).

[106] *See generally id.*

[107] *Specifications for Meta Pixel standard events*, FACEBOOK, https://www.facebook.com/business/help/402791146561655?id=1205376682832142 (last visited Mar. 18, 2026).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

when a user views pre-designated content, like products for sale (the "ViewContent" event);[108] and (iii) the "InitiateCheckout" event (collectively with PageView event, ViewContent event, the "Pixel Events").[109] The Website utilizes all three Pixel Events.[110]

149. When a User visited a webpage, including those with pre-recorded audio-visual materials, a PageView event and a ViewContent Event triggered, transmitting the item's title and content ID[111].

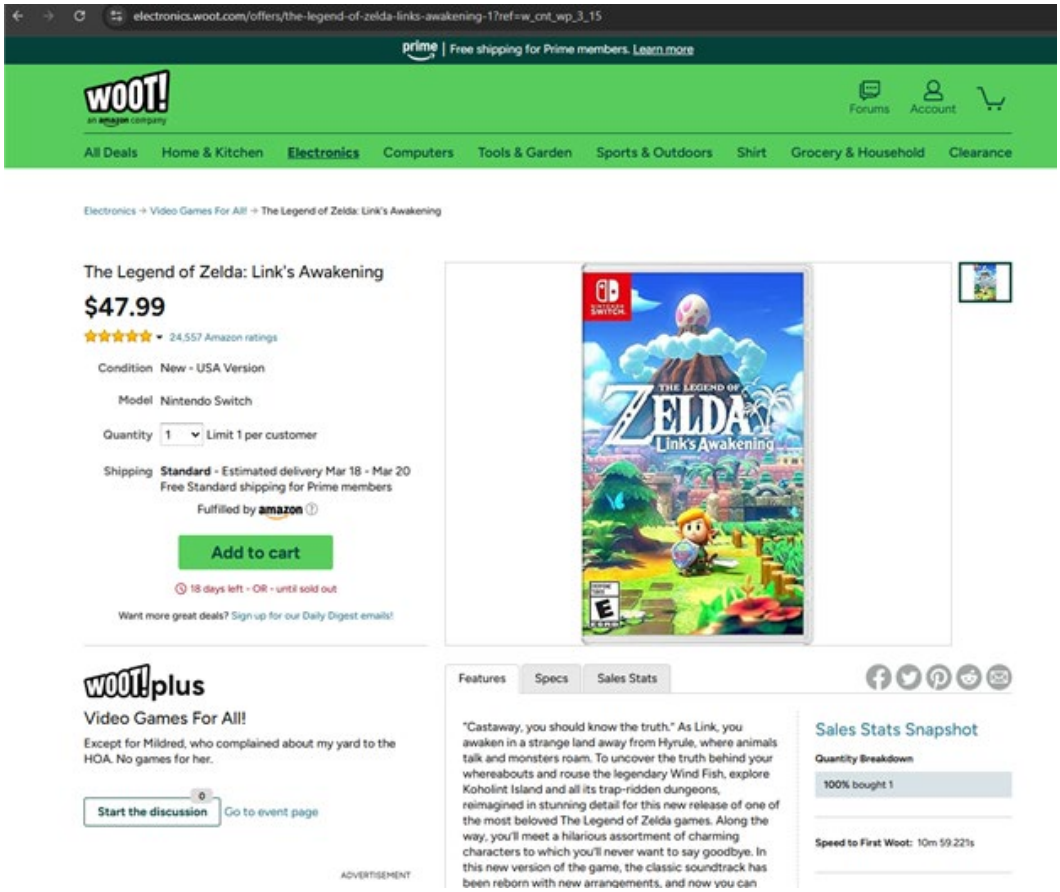
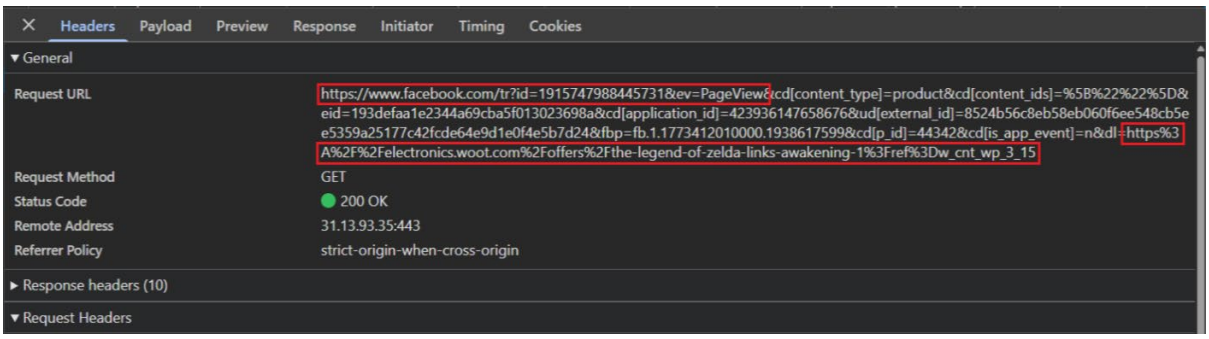


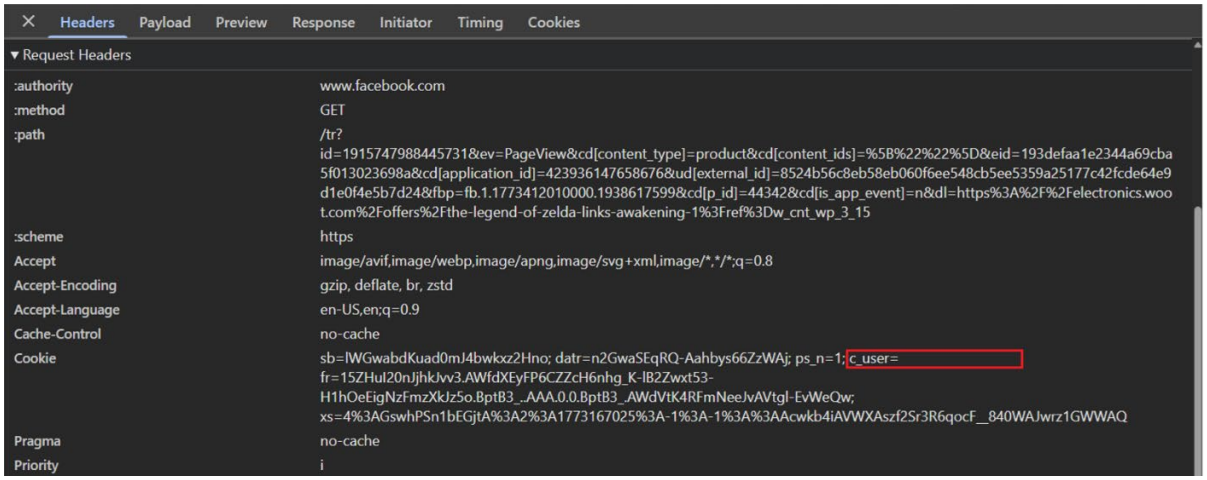

*Figure 9 – Sample webpage showcasing a product*

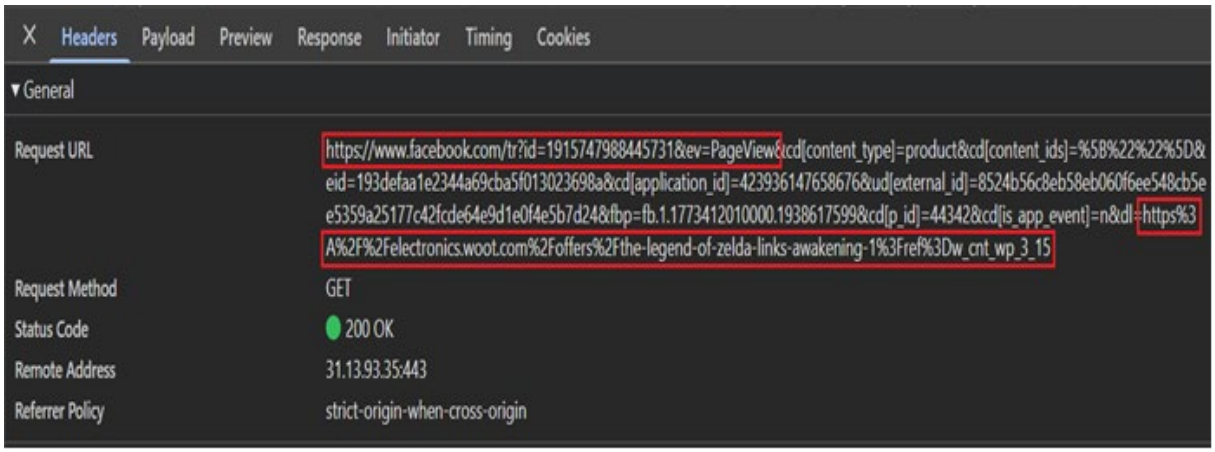
[108] *Reference: standard events*, FACEBOOK, https://developers.facebook.com/docs/meta-pixel/reference/ (last visited Mar. 19, 2026).
[109] *Id.*
[110] The presence of Pixel events can be confirmed by using the publicly available and free Meta Pixel Helper tool. *See About the Meta Pixel Helper*, FACEBOOK, https://www.facebook.com/business/help/198406697184603?id=1205376682832142 (last visited Mar. 19, 2026).
[111] The content ID is a number that is used by Woot to identify a specific product.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992






TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

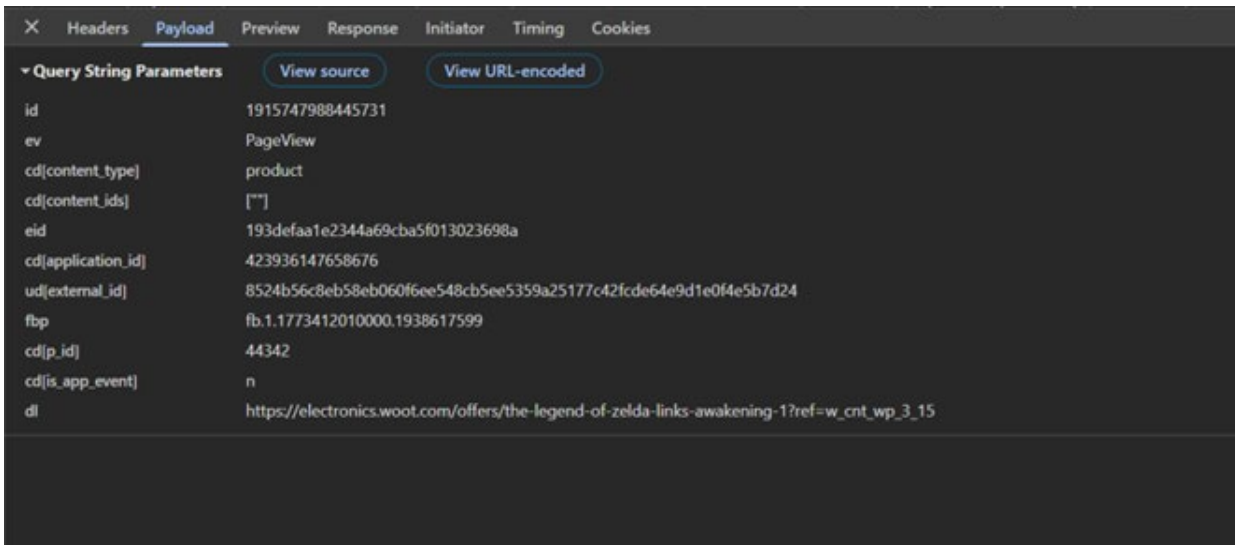
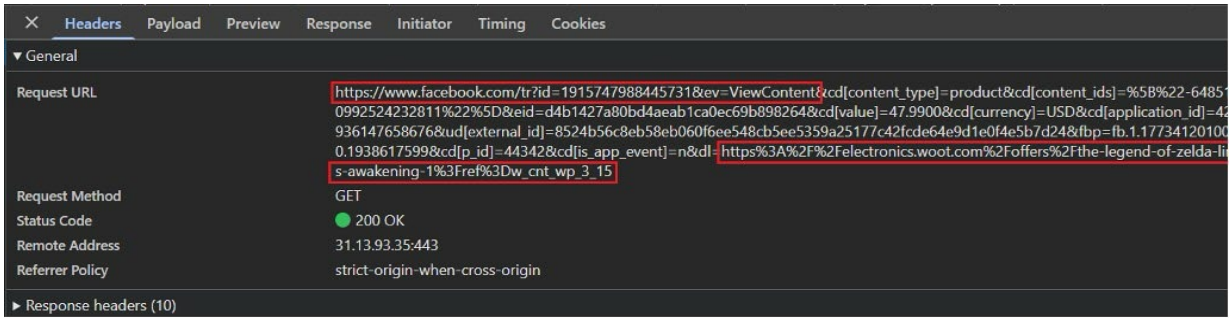
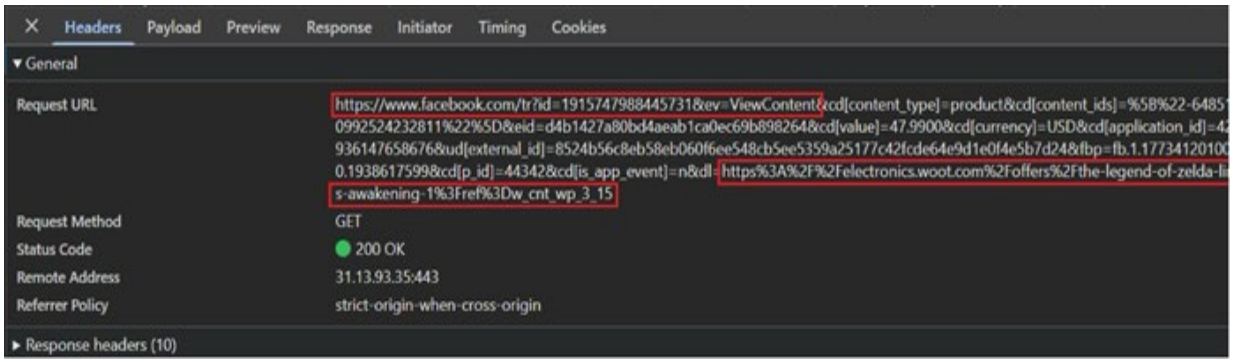



*Figure 10 – Meta Pixel tracking a User viewing the product from Figure 10 through the "PageView" event*






TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

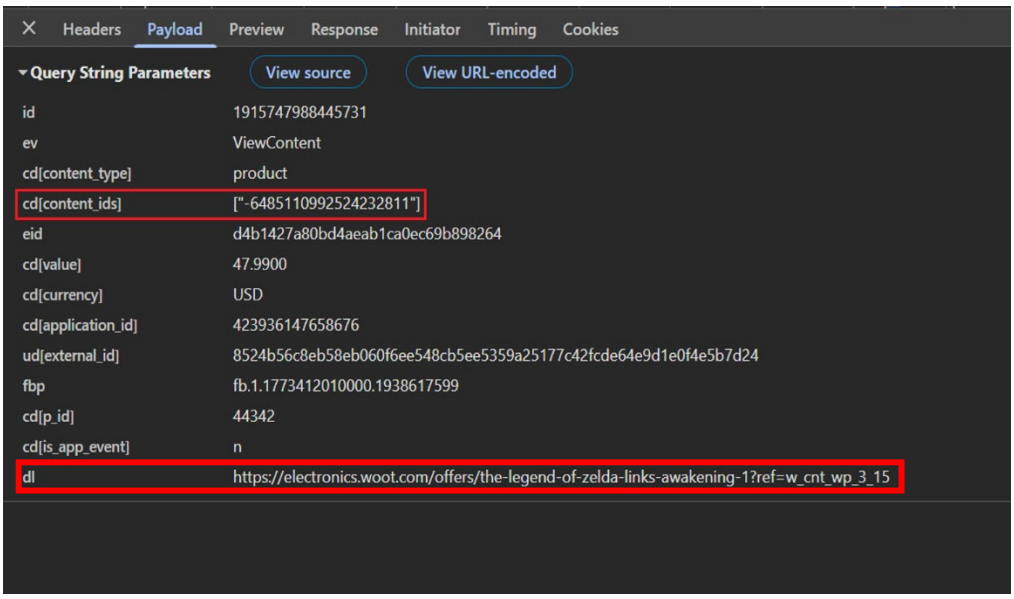



*Figure 11 – Facebook Meta Pixel tracking a User viewing the product from Figure 10 through the "ViewContent" event*

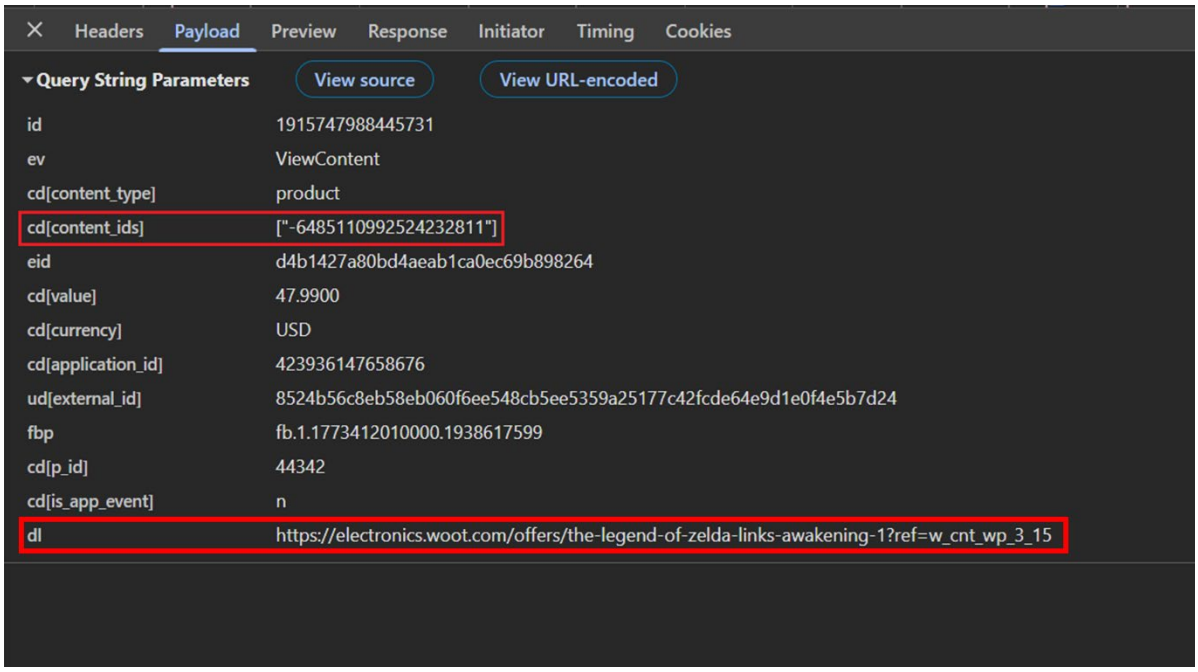



*Figure 12 – The payload from the "ViewContent" event, showing the content ID for the product from Figure 9*

150. The PageView event caused the User's browser to transmit data to Meta identifying the specific product page visited, including the product title contained within the requested URL and the content ID assigned to that product.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

151. When that same User viewed their shopping cart to initiate the checkout process, the Meta Pixel triggered an "InitiateCheckout" event that transmitted the same internal content identifier previously associated with the viewed product.

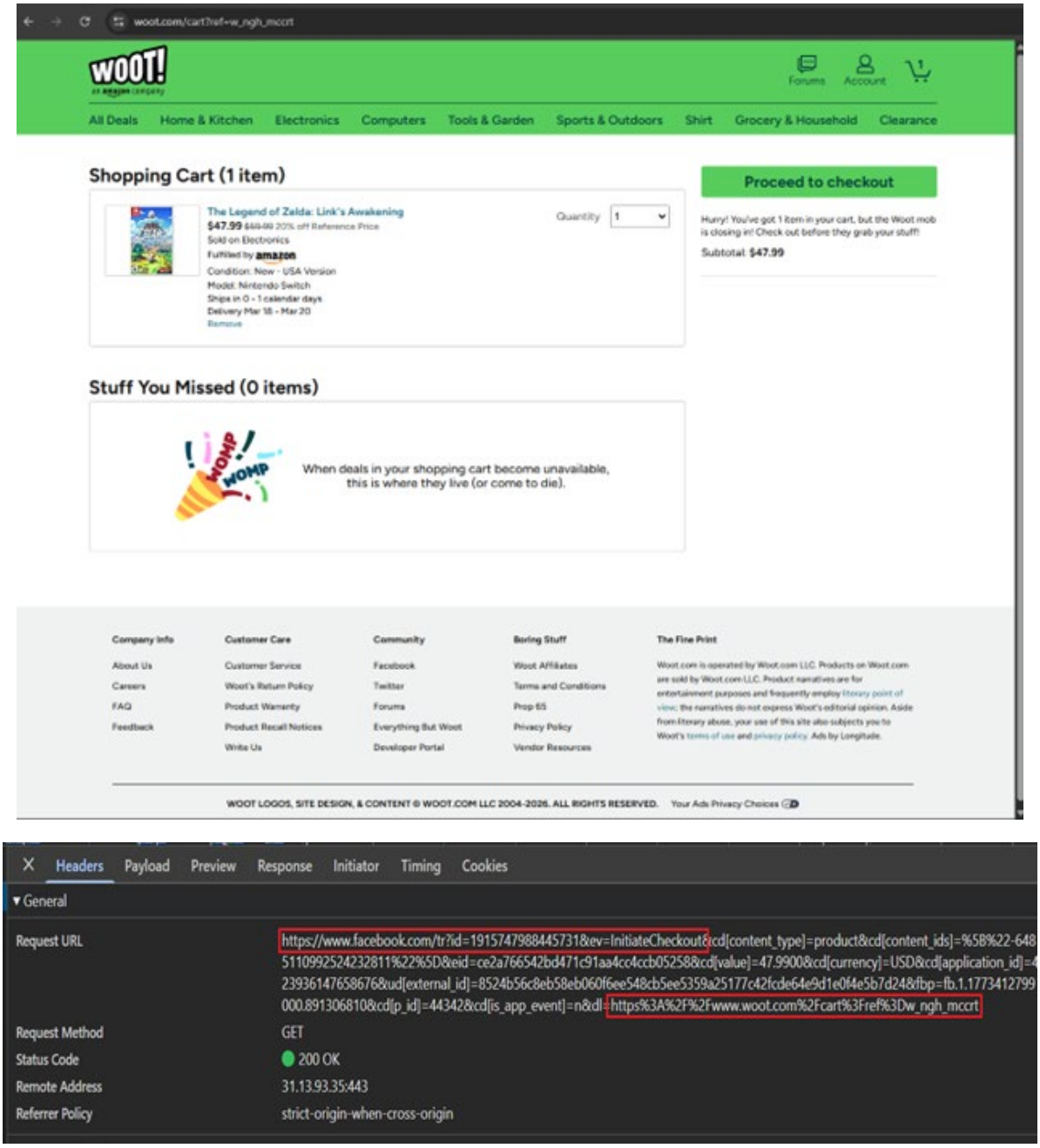



*Figure 13 - InitiateCheckout Meta Pixel event triggered when the User proceeds to checkout*



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

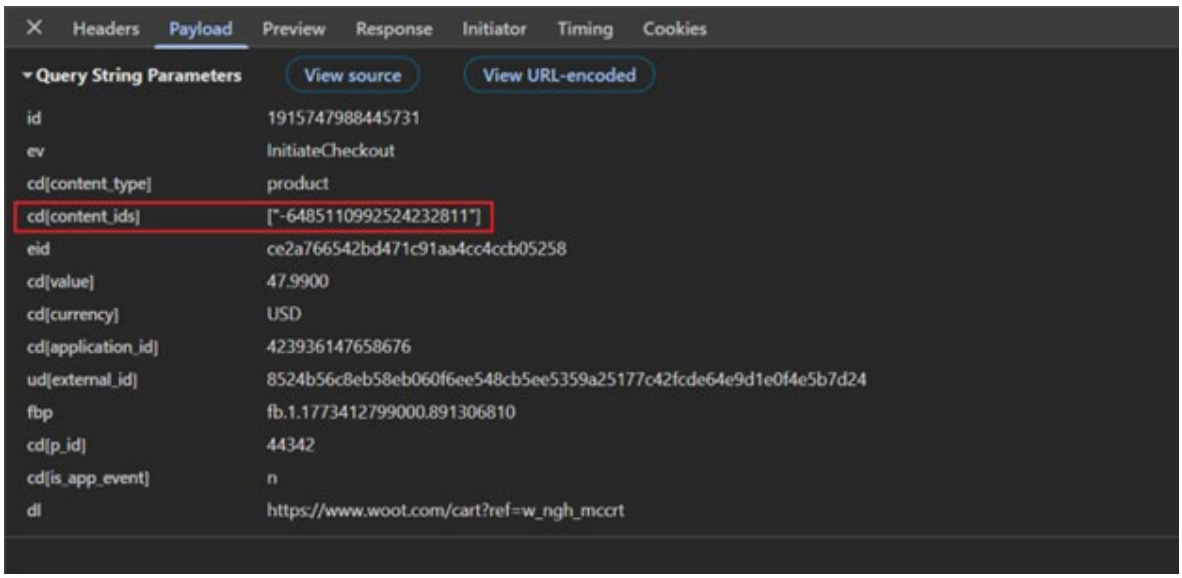



*Figure 14 – The payload from the "InitiateCheckout" event, showing the content ID for the product from Figure 9*

152. The ViewContent event disclosed the product name and the associated content ID to Meta. The InitiateCheckout event disclosed to Meta that the User is also a Purchaser purchasing a specific product, and identified the product using the previously disclosed Content ID. These two Meta Pixel events allow Meta to discover that a Purchaser is viewing a video game with a title associated with a content ID and subsequently purchasing an item with the same content ID, linking the title to the purchase. In short, the Meta Pixel Events implemented by Defendant allow Meta to ascertain Purchasers' identities and video game purchases through the c_user cookie, and to identify the products Purchasers are acquiring through the video game product's webpage URL and content ID.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

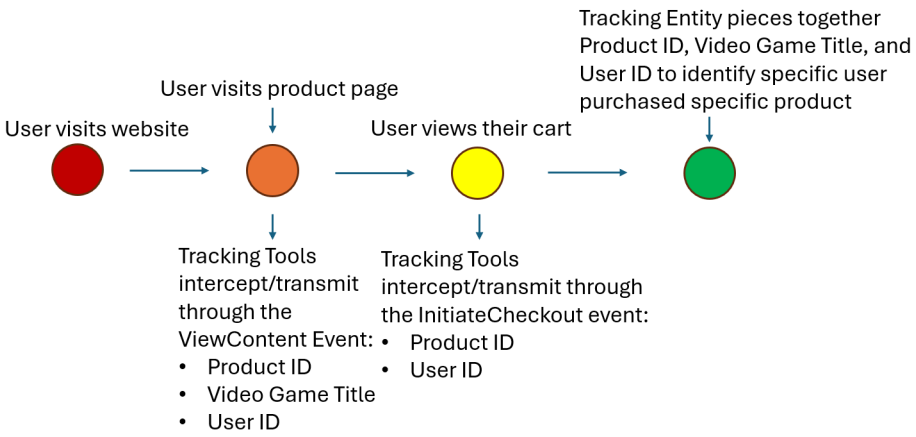



*Figure 15 – A graphic demonstrating the purchase information captured by the Meta Pixel*

153. When a Purchaser purchased pre-recorded audio-visual materials on the Website while logged into Facebook, the Website compelled a visitor's browser to transmit to Facebook the c_user cookie, which contained that visitor's unencrypted FID, along with other cookies like the datr, xs, fr, and ar_debug cookies, as shown in *Figure 18* below. The c_user, datr, and fr cookies allowed Meta to link purchases of video games featuring cut scenes to the Facebook user purchasing the pre-recorded audio-visual materials.[112] The event data disclosed by Defendant thus permits an ordinary person to identify the Purchaser through these cookies.

[112] *See Cookie Policy*, BMW, https://bavarianmotorcars.com/en/cookie-policy (last visited May 20, 2025); *See Cookie Policy*, BMW, https://bavarianmotorcars.com/en/cookie-policy (last visited May 20, 2025); *Common cookies and uses*, FACEBOOK, https://www.facebook.com/privacy/policies/cookies/?annotations[0]=explanation%2F1_common_cookies_and_uses (last visited May 20, 2025).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

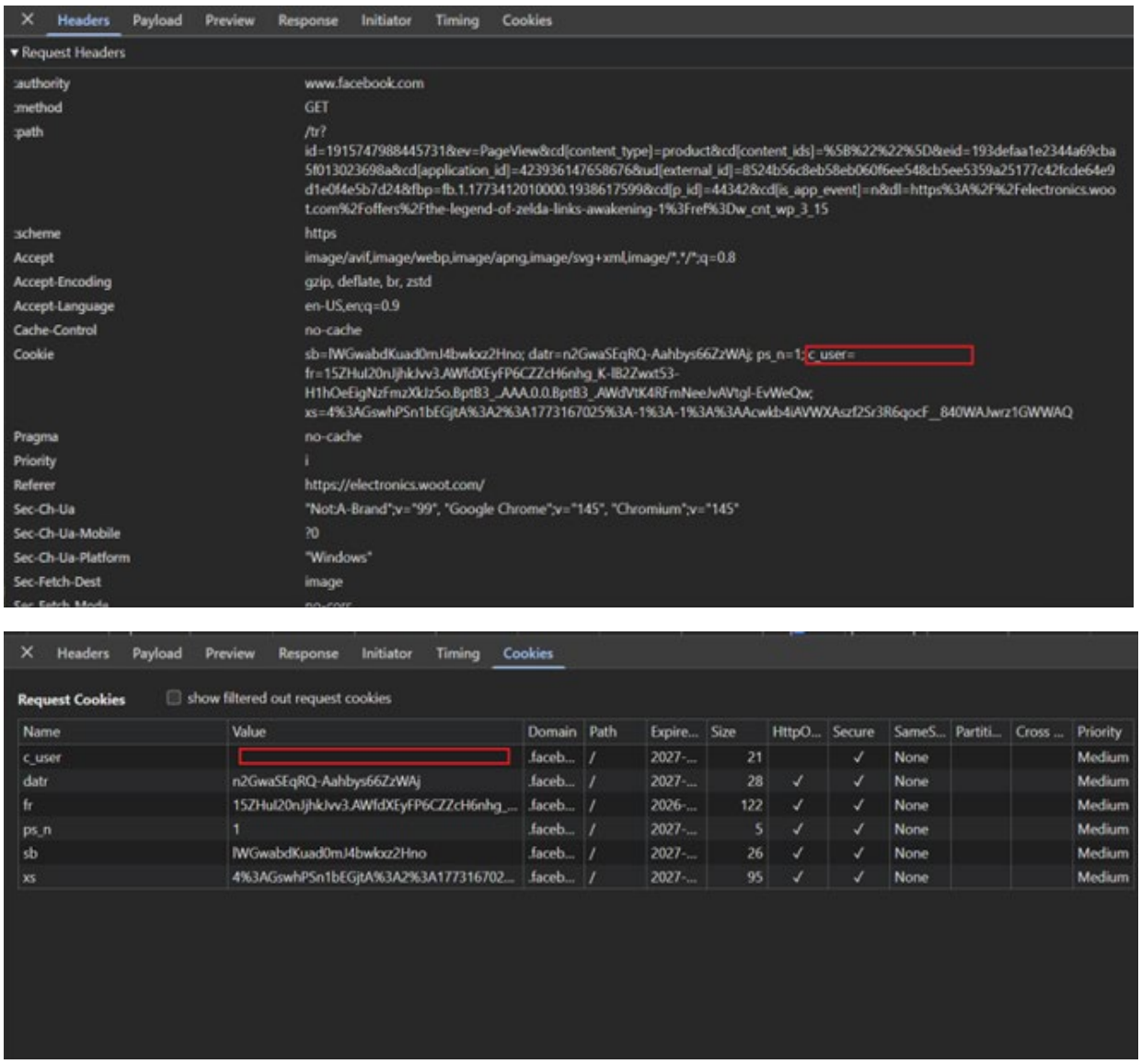



*Figure 16 – Cookies attached to Meta Pixel transmission*

154. Meta, at a minimum, uses the c_user, datr, and fr cookies to link to FIDs and corresponding Facebook profiles.

155. Meta admits that "[website owners] provide us with information about [their] existing customers and we match this information with Facebook profiles."[113] The customer lists must contain "'identifier[s]' (such as email, phone number, address)"[114] so that Meta can

[113] *Create a Customer Audience List*, FACEBOOK, https://www.facebook.com/business/help/170456843145568?id=24690979533764 (last visited Mar. 19, 2026).
[114] *Id.*



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

match the lists to "Facebook profiles" and "[website owners] can advertise to [their] customers on Facebook, Instagram, and Audience Network."[115]

156. While the technical evidence in this case may show the code-based transmission of an FID and a video title, Meta would not need to read or interpret that code manually. Instead, it receives and processes the information through internal systems that automatically extract the meaning of the data, linking a specific user to a specific video, with ease and accuracy.

157. Meta maintains an internal user interface that automatically translates incoming Meta Pixel transmissions into readable, plain-text formats. These interfaces allow Meta to view and analyze incoming data in human-understandable terms, such as here, identifying which user watched which video. Although these internal tools are not publicly available, their existence is evidenced by Meta's technical documentation and operational capabilities, which rely on the ingestion and automated interpretation of Meta Pixel data to serve ads and build user profiles.

158. Meta stores this broken-down, incoming Meta Pixel transmission data in its data warehouse, called the "Hive," and can analyze it to identify data sources and the contents of the transmitted data.[116]

159. Said differently, Meta designed the Meta Pixel transmission and reception capabilities to understand who is sending it data via the Meta Pixel and, further, what the event data means.

---

[115] *Customer List Custom Audiences*, FACEBOOK, https://www.facebook.com/business/help/341425252616329?id=24690979533764 (last visited Mar. 19, 2026).

[116] *See* Defendant Meta Platforms, Inc.'s Opposition to Plaintiffs' Motion for Sanctions, *In re Meta Pixel Healthcare*, No. 3:22-cv-03580-WHO (N.D. Cal. Dec. 30, 2024), ECF No. 740.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

160. Indeed, even the website operators who implement the Meta Pixel, like Defendant, have access to dashboards and analytics tools that display Meta Pixel outputs in clear, non-technical terms.

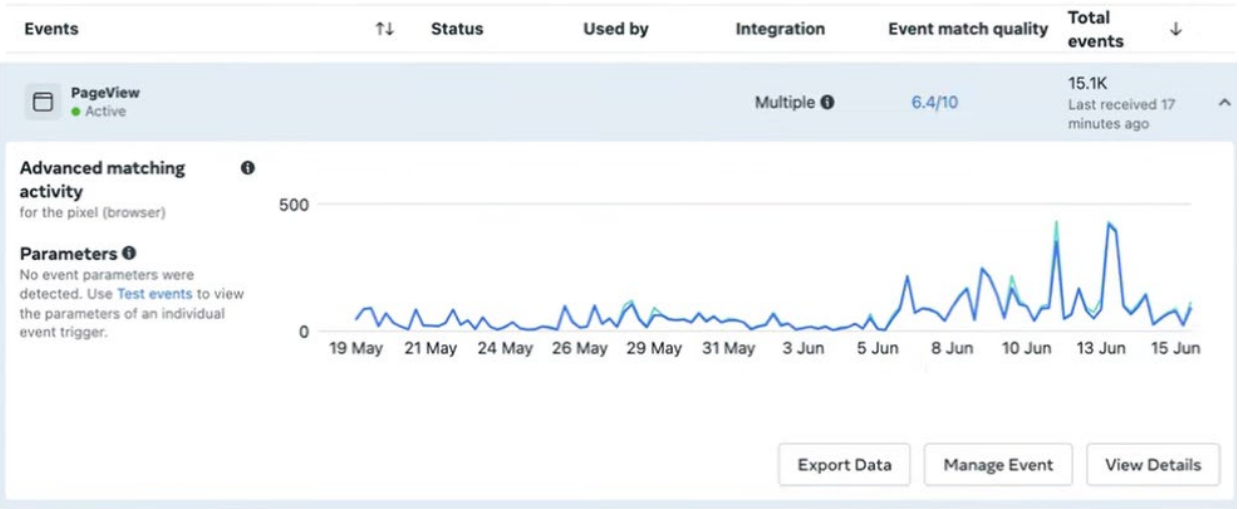



*Figure 17 – Meta Pixel outputs received from a third party's Event Manager for illustrative purposes*

161. These tools confirm that both Meta and its business partners interpret the underlying code using accessible interfaces designed to reveal user behavior in plain English.

162. Figure 17 shows, for example, how many PageView events were triggered in a given time frame, along with the parameters used to better match Users to their Facebook profiles.[117]

163. The dashboard will inform website operators of their event match quality—the better the event match quality, the more likely Meta Pixel events are being matched to Facebook profiles.[118]

164. Defendant, therefore, disclosed PII under the VPPA because the information transmitted to Meta—including Purchasers' FIDs and specific pre-recorded audio-visual material names (i.e., Personal Video Information)—was disclosed in a technical format, but one

[117] *See About event match quality*, META, https://www.facebook.com/business/help/765081237991954?id=818859032317965 (last visited Mar. 19, 2026).
[118] *Id.*



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

that is understood by ordinary people once removed from the technical encoding necessary to transmit the data. Much like a person does not understand raw radio waves to hear the sounds carried by the raw radio waves, one still understands the words coming out of the radio once the signal is received and processed by the radio.

### E. Woot Was Told that the Pixel Meta Discloses Users' Data; Woot Knew Precisely What the Meta Pixel Would Collect and Share

165. When a business applies with Meta to use the Meta Pixel, it is provided with details about its functionality (site policy).[119]

166. To make use of the Meta Pixel, Defendant agreed to Meta's Business Tool Terms (the "Business Terms").

167. The Business Terms inform website owners using Meta's tracking tools that the employment of the Meta Pixel will result in data sharing, including with Meta, through the automatic sharing of Meta Pixel Event Data and Contact Information.[120]

168. The Business Terms are transparent that the Event Data and Contact Information will be processed "... to match the Contact Information against user IDs ("Matched User IDs"), as well as to combine those user IDs with corresponding Event Data."[121]

169. Meta directs parties implementing the Meta Pixel – here, Woot– to encrypt request information[122] *before* data can be shared.[123]

---

[119] See *Get Started*, FACEBOOK https://developers.facebook.com/docs/meta-pixel/get-started (last visited Mar. 19, 2026) (The Pixel "relies on Facebook cookies, which enable us to match your website visitors to their respective Facebook User accounts. Once matched, we can their actions in the Facebook Ads Manager so you can use the data . . . By default, the Pixel will track URLs visited [and] domains visited . . . .").

[120] *Meta Business Tools Terms*, FACEBOOK, https://www.facebook.com/legal/terms/businesstools?paipv=0&eav=AfakosFmNyhZJOrkCsGodnMzth_uq6s403DsPEkeiKEyrj7rKyf5_t2I8wFEEUZUJlI&_rdr (last visited Mar. 19, 2026); see § C(1).

[121] *Id.*

[122] This contrasts with Facebook's JavaScript Pixel, which automatically encrypts the data being sent. Woot has specifically chosen the Pixel method which makes Users' information visible. *See id.*

[123] *Meta Business Tools Terms*, FACEBOOK, https://www.facebook.com/legal/terms/businesstools?paipv=0&eav=AfakosFmNyhZJOrkCsGodnMzth_uq6s403DsPEkeiKEyrj7rKyf5_t2I8wFEEUZUJlI&_rdr (last visited Mar. 19, 2026).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

170. Meta further provides website developers who implement the Meta Pixel, such as Woot, guidance on responsible data handling, and details on how data is acquired, used, and stored, including which information it would be sharing with Meta.

171. The Business Terms specifically require website developers who implement the Meta Pixel to represent and warrant that they will not share data that includes "sensitive information (including any information defined as sensitive under applicable laws, regulations, and applicable industry guidelines)."[124]

172. Meta educates or reminds website developers who implement the Meta Pixel of their responsibility to inform Meta Pixel users of their websites' data sharing, and specifically guides website owners to obtain the requisite rights, permissions, or consents before sharing information with any third parties.[125]

173. Aside from Meta informing Defendant that it needed "a clear and prominent notice on each web page where [its] Pixels are used[,]" Defendant was also on notice that it must "ensure, in a verifiable manner, that an end user provide[d] all necessary consents before [Woot] use[d] [Meta's Pixel] to enable the storage of and access to Meta cookies . . . [i]n jurisdictions that require informed consent."[126]

174. As a sophisticated party entering into a business arrangement with another sophisticated party, Woot was on notice of the potential privacy violations that would result from the Website's use of the Meta Pixel, and ignored Meta's warnings to safely handle and protect Users' data and/or to warn Purchasers that the Website would disclose information in a manner that threatened Purchasers' VPPA-protected Personal Video Information.

---

[124] *Id.*

[125] *Best practices for privacy and data use for Meta Business Tools*, FACEBOOK, https://www.facebook.com/business/help/363303621411154?id=818859032317965 (last visited Mar. 19, 2026).

[126] *Id.*



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

## III. The Website Lacks Informed, Written Consent Separate and Distinct from Other Obligations, Pursuant to the VPPA

175. The Website does not seek nor obtain permission from Purchasers, including Plaintiffs and the Class Members, to share Purchasers' Personal Video Information with Tracking Entities, including Meta.

176. To the extent information about any of the Website's data sharing can be located, the language is not (i) presented to Purchasers of the site in a transparent manner, or where it must be viewed by Purchasers; (ii) made available as part of the sign-up process; (iii) offered to Purchasers as checkbox or e-signature field, or as any form of consent; and (iv) presented in terms that sufficiently warn Purchasers that their information, protected by the VPPA, will be shared with Meta.[127]

177. Woot's Privacy Policy does not disclose the use of Tracking Tools by the Tracking Entities.[128] Amazon's Privacy Notice, which Woot links to in its own Privacy Policy, only briefly mentions the use of cookies and does not disclose the use of third-party Tracking Tools.[129] Amazon's Cookie Notice, which Amazon links to in its Privacy Notice, does disclose the use of Tracking Tools but does not disclose what data they collect.[130] None of these documents discloses that Meta is one of the Tracking Entities.

178. The VPPA has specific requirements for how written and informed consent must be given. Generic references in Defendant's Privacy Policy to the use of cookies and potential third-party data sharing do not equate to the explicit, informed consent required under the VPPA. *See* 18 U.S.C. § 2710(b)(2)(B).

179. Consent under the VPPA also "require[s] video tape service providers to request Users' consent to a privacy disclosure that addresses only the use of [Personal Video

---

[127] *See Privacy Policy*, WOOT, https://www.woot.com/privacy?ref=w_ngf_pp (last visited Mar. 19, 2026).
[128] *Id.*
[129] *See Privacy Policy*, AMAZON, https://www.amazon.com/gp/help/customer/display.html/ref=hp_left_v4_sib?nodeId=GX7NJQ4ZB8MHFRNJ&ie=UTF8&ref_=hp_left_v4_sib (last visited April 27, 2026).
[130] *See Cookies*, AMAZON, https://www.amazon.com/gp/help/customer/display.html/?nodeId=GVASXV5UZ64R4Y25 (last visited April 27, 2026).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Information] . . . and no other privacy topic . . . ." *See Cappello v. Walmart Inc.*, No. 18-cv-06678-RS, 2019 WL 11697705, at *2 (N.D. Cal. Apr. 5, 2019).

180. Defendant's broad Privacy Policy does not expressly authorize the precise form of Personal Video Information at issue here. Defendant, therefore, did not obtain Purchasers', including Plaintiffs', VPPA-required consent.

181. At the time of purchase, Purchasers simultaneously assent to the Terms of Use and Privacy Policy through a single button click.

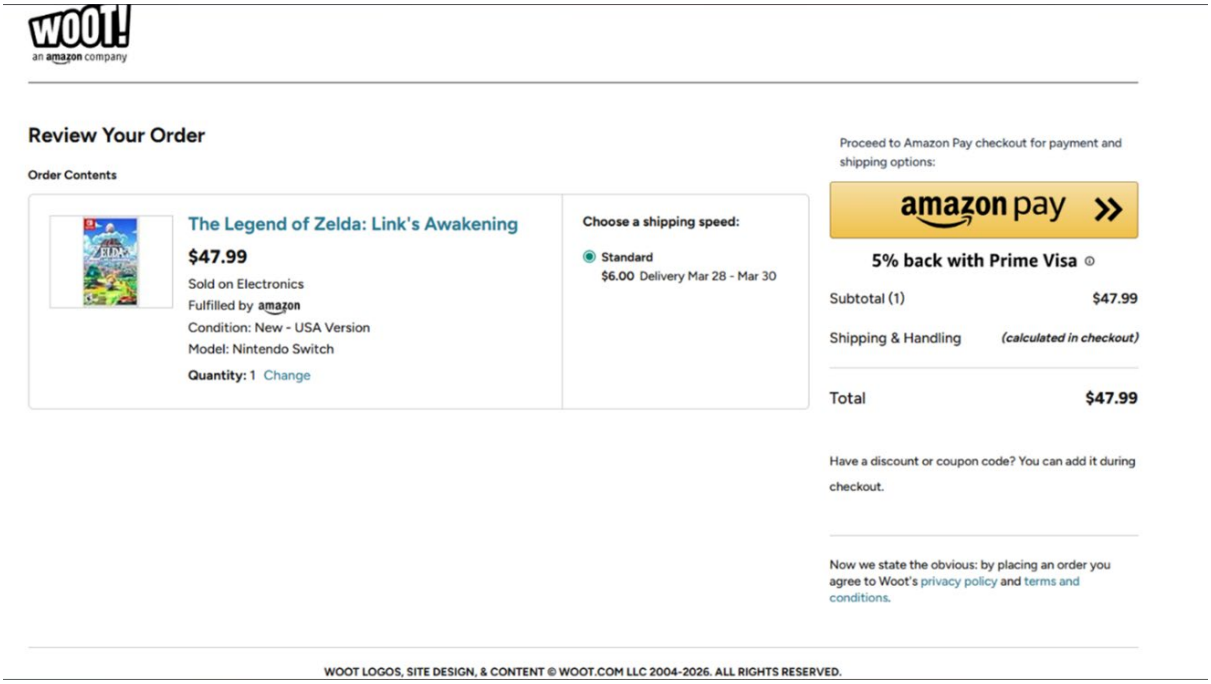



*Figure 18 – Checkout page on the Website where Purchasers agree to the Privacy Policy and the Terms of Use at the same time*

182. In the Terms of Use, Purchasers agree to receive communications electronically, are granted a license for use of the Website, accept risk of loss and title upon delivery of products to a carrier, agree to Coupon terms, agree to the law of the State of Washington, and agree to bring disputes in King County, Washington, among other legal obligations.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

183. Defendant therefore never obtains consent from Purchasers in a form that is "distinct and separate from any form setting forth other legal or financial obligations of the consumer." *See* 18 U.S.C. § 2710(b)(2)(B)(i).

## IV. Plaintiffs Did Not Consent to Defendant's Sharing of Plaintiffs' Sensitive Information

184. Plaintiffs and the Class Members were unaware that the Tracking Tools intercepted their communications in the form of their browsing history.

185. Plaintiffs and the Class Members reasonably believed that communications to the Website were made in confidence.

186. With no notice or warning as to who was intercepting and decoding the contents of their communications, Plaintiffs were not provided notice of or given an opportunity to provide consent to the Meta Pixel's and other Tracking Tools' interceptions of Plaintiffs' Sensitive Information.

187. Meta instructs and cautions website operators about the legal risks of using their Tracking Tools without first providing adequate notice and obtaining valid consent for the invasive collection of Users' protected data. These companies also warn against making such data available to Tracking Entities or enabling its interception. Indeed, Meta expressly requires website operators to agree not to transmit Users' sensitive data—even if consent is purportedly obtained. Defendant accepted these terms as a condition of deploying the Tracking Tools on its Website.

188. Plaintiffs were not given notice of the use of the Tracking Tools on the Website.

189. As a result, Plaintiffs did not and could not provide consent to the collection and sharing of their Sensitive Information when visiting the Website, browsing products on the Website, and purchasing pre-recorded audio-visual materials on the Website.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

## TOLLING

190. The statutes of limitations applicable to Plaintiffs' and the Class Members' claims were tolled by Defendant's conduct and Plaintiffs' and the Class Members' delayed discovery of their claims.

191. As alleged above, Plaintiffs and the Class Members did not know, and could not have known, that when they used the Website, Defendant was disclosing their Sensitive Information to Tracking Entities. Plaintiffs and the Class Members could not have discovered Defendant's unlawful conduct with reasonable diligence.

192. Defendant secretly incorporated the Tracking Tools into the Website, providing no indication to Users that their Sensitive Information would be intercepted and disclosed to the Tracking Entities.

193. Defendant had exclusive and superior knowledge that the Tracking Entities' Tracking Tools, incorporated on its Website, would disclose Users' Sensitive Information, yet failed to disclose to Users that by interacting with the Website, Plaintiffs' and the Class Members' Sensitive Information would be disclosed to the Tracking Entities.

194. Plaintiffs and the Class Members could not, with due diligence, have discovered the full scope of Defendant's conduct because the incorporation of the Tracking Entities' tracking tools is highly technical, and there were no disclosures or other indications that would inform a reasonable consumer or Website User that Defendant was disclosing and allowing the interception of such information to Tracking Entities.

195. The earliest that Plaintiffs and the Class Members could have discovered Defendant's conduct was through their investigation and the work performed on their behalf in preparation for filing this Complaint.

## CLASS ACTION ALLEGATIONS

196. Plaintiffs bring this action individually and on behalf of the following Class and Subclasses:



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

**Class:** All natural persons in the United States who used Defendant's Website during the applicable limitations period and whose electronic communications were intercepted, disclosed, and/or transmitted to the Tracking Entities through Defendant's Website's use of the Tracking Tools (the "Class").

**California Subclass:** All members of the Class who visited and interacted with Defendant's Website during the applicable limitations period while located in the State of California (the "California Subclass").

**Florida Subclass:** All members of the Class who visited and interacted with Defendant's Website during the applicable limitations period while located in the State of Florida (the "Florida Subclass")

**VPPA Subclass:** All members of the Class who purchased pre-recorded audio-visual materials through Defendant's Website during the applicable limitations period (the "VPPA Subclass").

197. Specifically excluded from the Class and Subclasses are Defendant, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint venturers, or entities controlled by Defendant, and its heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

198. Plaintiffs reserve the right to amend the Class and Subclass definitions above if further investigation and/or discovery reveals that the Class or Subclasses should be expanded, narrowed, further divided into subclasses, or otherwise modified in any way.

199. This action may be certified as a class action under Federal Rule of Civil Procedure 23 because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

200. Numerosity (Rule 23(a)(1)): At this time, Plaintiffs do not know the exact number of members of the aforementioned Class and Subclasses. However, given the popularity of Defendant's Website, the number of persons within the Class is believed to be so numerous that joinder of all members is impractical.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

201. Typicality of Claims (Rule 23(a)(3)): Plaintiffs' claims are typical of those of the Class and Subclasses because Plaintiffs, like all Class and Subclass Members, used the Website, purchased pre-recorded audio-visual materials on the Website, and had their Sensitive Information intercepted and transmitted via the Website's Tracking Tools.

202. Adequacy of Representation (Rule 23(a)(4)): Plaintiffs will fairly and adequately represent and protect the interests of the Class. Plaintiffs have no interests antagonistic to, nor in conflict with, the individual members of the Class. Plaintiffs have retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

203. Superiority (Rule 23(b)(3)): A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class and Subclass Members are relatively small, the expense and burden of individual litigation make it impossible for individual Class and Subclass Members to seek redress for the wrongful conduct asserted herein. If class treatment of these claims is not available, Defendant will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

204. Commonality and Predominance (Rule 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 and Subclasses that predominate over questions that may affect individual members of the Class and Subclasses include:

a. Whether Defendant violated Plaintiffs' and the Class Members' privacy rights;

b. Whether Defendant's acts and practices violated the VPPA;

c. Whether Defendant's acts and practices violated the Wiretap Act;

d. Whether Defendant's acts and practices violated CIPA;

e. Whether Defendant's acts and practices violated the FSCA;



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

f. Whether Plaintiffs and the Class Members are entitled to equitable relief, including, but not limited to, injunctive relief; and

g. Whether Plaintiffs and the Class Members are entitled to statutory or other forms of damages, and other monetary relief.

205. Information concerning Defendant's Website's data sharing practices is available from Defendant's or third-party records.

206. Plaintiffs know of no difficulty that will be encountered in the management of this litigation that would preclude its maintenance as a class action.

207. The prosecution of separate actions by individual Class Members would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendant. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

208. Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

209. Given that Defendant's conduct is ongoing, monetary damages are insufficient, and there is no complete and adequate remedy at law.

## CAUSES OF ACTION

### COUNT I
### VIOLATIONS OF THE VIDEO PRIVACY PROTECTION ACT
### 18 U.S.C. § 2710
### (On Behalf of Plaintiffs and the VPPA Subclass)

210. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above as though fully set forth herein.

211. Plaintiffs bring this count on behalf of themselves and all members of the VPPA Subclass.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

212. The VPPA provides that "a video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer shall be liable to the aggrieved person for" "actual damages but not less than liquidated damages in an amount of $2,500," punitive damages, reasonable attorneys' fees and costs, as well as "such other preliminary and equitable relief as the court determines to be appropriate." 18 U.S.C. §§ 2710(b)(1), 2710(c)(2).[131]

213. "Personally identifiable information" is defined to include "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).

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

215. Defendant violated the VPPA by knowingly disclosing Plaintiffs' and other VPPA Subclass Members' Personal Video Information to Meta.

216. Defendant, through the Website, engages in the business of delivering pre-recorded audio-visual materials to Purchasers, including Plaintiffs and the other VPPA Subclass Members. The Website delivers pre-recorded audio-visual materials to Purchasers, including Plaintiffs and the other VPPA Subclass Members, by selling those materials, including in the form of video games that include cut scenes, to Plaintiffs and the other VPPA Subclass Members on the Website.

217. Defendant is a "video tape service provider" because it curates, hosts, and sells pre-recorded audio-visual materials on the Website, thereby "engag[ing] in the business, in or

[131] 18 U.S.C. § 2710(b)(1) refers to "relief provided in subsection (d)"; however, "[t]his appears to be a typo, because subsection (d) is a rule of evidence which renders inadmissible personally identifiable information, whereas subsection (c) describes the remedies available to a VPPA plaintiff in a civil action." *In re Nickelodeon Consumer Privacy Litig.*, No. 2443 (SRC), 2014 U.S. Dist. LEXIS 91286, at *22 n.7 (D.N.J. July 2, 2014) (citing *Sterk v. Redbox Automated Retail, LLC*, 672 F.3d 535, 537 (7th Cir. 2012)).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

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).

218. Defendant qualifies as a "video tape service provider" under the VPPA. Defendant is in the business of selling pre-recorded audio-visual materials.

219. Plaintiffs and the VPPA Subclass Members are "purchasers" because they purchased pre-recorded audio-visual materials from Defendant's Website. *See* 18 U.S.C. § 2710(a)(1).

220. Plaintiff Roth purchased Pokemon Scarlet and Tales of Graces f Remastered from Defendant. Pokemon Scarlet and Tales of Graces f Remastered are prerecorded video content because they contain prerecorded video cutscenes.[132]

221. Plaintiff Rose purchased Metroid Prime 4 Beyond and Donkey Kong Country Returns HD from Defendant. Metroid Prime 4 Beyond and Donkey Kong Country Returns HD are prerecorded video content because they contain prerecorded video cutscenes.[133]

222. Plaintiff Fonseca purchased Dragon Ball: Sparking! Zero from Defendant. Dragon Ball: Sparking! Zero is prerecorded video content because it contains prerecorded video cutscenes.[134]

---

[132] *Pokemon Scarlet and Violet Fans Put Voice Acting Into Key Cutscenes*, GAMERANX (Nov. 30, 2022) https://gameranx.com/updates/id/408362/article/pokemon-scarlet-and-violet-fans-put-voice-acting-into-key-cutscenes/ (last visited Mar. 24, 2026); *Pokémon Scarlet & Violet - All Cutscenes (REUPLOAD)*, YOUTUBE, https://www.youtube.com/watch?v=y6sYZWpk7Uw (last visited Mar. 24, 2026); *What's New in Tales of Graces f Remastered?*, BANDAI NAMCO (Jan. 21, 2025), https://www.nintendo-insider.com/tales-of-graces-f-remastered-review/ (last visited Mar. 24, 2026); *Tales of Graces f Remastered Review*, NINTENDO INSIDER (September 23, 2024), https://en.bandainamcoent.eu/tales-of/news/whats-new-tales-of-graces-f-remastered (last visited Mar. 24, 2026); *Tales of Graces f Remastered ★ THE MOVIE / ALL CUTSCENES 【Cinematic Edition / No Skits】*, YOUTUBE, https://www.youtube.com/watch?v=eV1O-b2wPdU (last visited Mar. 24, 2026)..

[133] *METROID PRIME 4 BEYOND All Cutscenes (Full Game Movie) 4K 60FPS Ultra HD*, YOUTUBE, https://www.youtube.com/watch?v=WwFzVhlYhMw (last visited Apr. 21, 2026); Metroid Prime 4 Beyond - All Cutscenes [Full Movie] (4K), YOUTUBE, https://www.youtube.com/watch?v=ikM8wGEbhE4 (last visited on April 21, 2026); *Donkey Kong Country Returns HD - All Cutscenes*, YOUTUBE, mhttps://www.youtube.com/watch?v=WipcSnXBeyQ (last visited Apr. 21, 2026).

[134] *Dragon Ball: Sparking! Zero*, BANDAI NAMCO, https://en.bandainamcoent.eu/dragon-ball/dragon-ball-sparking-zero (last visited on March 18, 2026); *DRAGON BALL SPARKING ZERO All Cutscenes (Full Game Movie) 4K 60FPS Ultra HD* , YOUTUBE, https://www.youtube.com/watch?v=aDXncW1iUQg (last visited Mar. 18, 2026).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

223. Defendant, without disclosing to Purchasers or seeking consent, surreptitiously shared Plaintiffs' and the VPPA Subclass Members' Personal Video Information to Meta. Defendant utilized the Meta Pixel, which forced Plaintiffs' web browsers to transmit Plaintiffs' Personal Video Information, like their FIDs, along with Plaintiffs' and the VPPA Subclass Members' event data, including the title of the pre-recorded audio-visual materials they purchased, to Meta.

224. Defendant knowingly disclosed Plaintiffs' and the VPPA Subclass Members' Personal Video Information through its implementation of the Meta Pixel, which automatically triggers the capture and transmission of such data. Defendant was specifically informed by the Tracking Entities about how the Tracking Tools functioned, the scope of data collected, and their capability to link individual Purchasers to their activity on the Website. Once the Meta Pixel completes its automatic exchange, the resulting FID can be used by an ordinary person to readily identify a specific Facebook account holder. See Section III(C) (process to identify an individual using FID).

225. Plaintiffs and the VPPA Subclass Members did not provide Defendant with any form of consent—either written or otherwise—to disclose their Personal Video Information to Meta. Defendant failed to obtain "informed, written consent" from Purchasers "in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer" and "at the election of the consumer," either "given at the time the disclosure is sought" or "given in advance for a set period of time, not to exceed 2 years or until consent is withdrawn by the consumer, whichever is sooner." *See* 18 U.S.C. § 2710(b)(2)(B)(i)-(ii).

226. Defendant's disclosures of Plaintiffs' and the VPPA Subclass Members' Personal Video Information were not made in the "ordinary course of business" as the term is defined by the VPPA. Defendant's disclosure of Purchasers' Personal Video Information to Meta was not necessary for "debt collection activities, order fulfillment, request processing, [or] transfer of



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

ownership." 18 U.S.C. § 2710(a)(2). Instead, Plaintiffs' and the VPPA Subclass Members' Personal Video Information was used to improve marketing effectiveness and generate profit.

227. In addition, 18 U.S.C. § 2710(b)(2)(B)(iii) expressly enumerates an opt-out right for consumers, which requires video tape service providers like Defendant to "provide[] an opportunity for the consumer to withdraw on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer's election." Defendant failed to provide an opportunity for Plaintiffs and the VPPA Subclass Members to opt out as required by the VPPA.

228. On behalf of themselves and the VPPA Subclass Members, Plaintiffs seek: (i) declaratory relief as to Defendant; (ii) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the VPPA Subclass Members by requiring Defendant to comply with the VPPA's requirements for protecting consumers' Personal Video Information; (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.

***Injunctive Relief of Defendant's Ongoing Violations***

229. An actual and immediate controversy has arisen and now exists between Plaintiffs and the putative Class they seek to represent, and Defendant, which parties have a genuine and opposing interest in and whose interests are direct and substantial. Defendant has violated, and continues to violate, Plaintiffs' and the Class members' privacy rights.

230. Plaintiffs have demonstrated that they are likely to succeed on the merits of their claims and are thus entitled to declaratory and injunctive relief.

231. Plaintiffs have no adequate remedy at law to stop the continuing violations of the VPPA by Defendant. Unless enjoined by the Court, Defendant will continue to infringe on the privacy rights of Plaintiffs and the VPPA Subclass members, and will continue to cause, or allow to be caused, irreparable harm to Plaintiffs and VPPA Subclass members. Injunctive relief is in the public interest to protect the Personal Video Information of Plaintiffs and the VPPA Subclass



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

members that would be irreparably harmed through continued interception and/or disclosure of their Sensitive Information.

232. Defendant completely disregards its obligations under the VPPA by loading the Tracking Tools onto the Website and facilitating the sharing of Purchasers', i.e., Plaintiffs' and the VPPA Subclass members', Personal Video Information with Tracking Entities for any ordinary person to access and use.

233. Despite brazenly violating the VPPA, Plaintiffs and the VPPA Subclass members were provided with no notice of the employment of the Tracking Tools and no indication of how or how much of their information was shared with Tracking Entities. Worse, in further violation of the VPPA, Defendant did not seek or obtain any form of consent from Plaintiffs or the VPPA Subclass members for the Tracking Tools' interception, disclosure, and/or use of the Personal Video Information communicated to the Website.

234. This threat of injury to Plaintiffs and members of the VPPA Subclass arising from Defendant's continuous violations requires temporary, preliminary, and permanent injunctive relief to ensure that Plaintiffs' and the VPPA Subclass members' Personal Video Information is protected from future unauthorized disclosure.

## COUNT II
## COMMON LAW INVASION OF PRIVACY
### Intrusion Upon Seclusion
### (On Behalf of Plaintiffs and the Class)

235. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above as though fully set forth herein.

236. Plaintiffs bring this claim on behalf of themselves and all Class Members.

237. Plaintiffs and the Class Members maintained a reasonable expectation of privacy in their communications with Defendant via its Website. Users' search terms, browsing history,



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

geolocation data, and website activity have been recognized by society as sensitive information.[135]

238. Plaintiffs' and the Class Members' reasonable expectation of privacy is supported by, *inter alia*, the VPPA's recognition that their Personal Video Information is Sensitive Information that must be protected from unauthorized disclosure, as well as the Wiretap Act's prohibition against unauthorized interception of communications.

239. Plaintiffs and the Class Members maintained a reasonable expectation of privacy in believing that Defendant would not disclose their Sensitive Information to the Tracking Entities.

240. Further, Plaintiffs and the VPPA Subclass Members maintained a reasonable expectation of privacy in believing that Defendant, as a video tape service provider ("VTSP") under the VPPA, would not disclose their Personal Video Information, which includes searches for, viewing of, requests for, or acquisition of pre-recorded audio-visual materials.

241. Defendant had a duty to refrain from sharing such information absent explicit authorization from Users, which it failed to obtain.

242. Plaintiffs and the Class Members have an interest in: (i) precluding the dissemination and/or misuse of their Sensitive Information; and (ii) being free to visit and interact with internet websites without being subjected to wiretaps without Plaintiffs' and/or the Class Members' knowledge or consent.

243. Plaintiffs and the Class Members possessed a reasonable expectation of privacy based on the belief that Defendant would abide by applicable state and federal laws, such as the Wiretap Act and CIPA. CIPA prohibits Tracking Entities from intercepting communications between Users, like Plaintiffs and the Class Members, and Defendant's Website without the

[135] For example, California voted to pass the California Consumer Privacy Act of 2018, and voted to amend it in 2020 through Proposition 24, the California Privacy Rights Act (CPRA). The CPRA sets out that colling and using "personal information," including real names, online identifiers, internet browsing and search history, location data, audio and visual information, etc., requires businesses to provide adequate notice of such practices. See *generally* Cal. Civ. Code §§1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.140(v).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

consent of all parties involved in the communication. Through its placement of Tracking Tools on the Website, Defendant enabled this interception and resulting intrusion upon Plaintiffs' and Class Members' privacy.

244. As explained above, Defendant's actions constitute a serious invasion of privacy that was an egregious breach of social norms, such that the breach was highly offensive to a reasonable person because:

a. the invasion of privacy occurred in a highly sensitive setting – Plaintiffs' communications with Defendant (applicable to the VPPA Subclass members, Defendant is a VTSP);

b. Defendant had no legitimate objective or motive in invading Plaintiffs' and the Class Members' privacy in such a manner;

c. Defendant violated multiple laws by invading Plaintiffs' and Class Members' privacy, including the Wiretap Act and CIPA;

d. Defendant deprived Plaintiffs and Class Members of the ability to control dissemination of their Sensitive Information; and

e. With respect to the VPPA Subclass Members, Defendant's actions are also unacceptable as a matter of public policy because they undermine the relationship between Purchasers of prerecorded audio-visual materials and their VTSPs.

245. During the relevant time period, Defendant intentionally invaded the privacy rights of Plaintiffs and Class Members by implementing Tracking Tools on its Website and actively enabling the Tracking Entities to collect and intercept their sensitive and confidential information.

246. As a direct and proximate result of this infringement upon their privacy, Plaintiffs and the Class Members sustained harm and experienced various damages. In light of this injury, Plaintiffs and Class Members are pursuing suitable remedies, such as compensatory damages,



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

restitution, disgorgement, punitive damages, and any other relief that the Court deems appropriate and fair.

**COUNT III**
**VIOLATIONS OF THE FEDERAL WIRETAP ACT**
**18 U.S.C. § 2510, et seq.**
**(On Behalf of Plaintiffs and the Class)**

247. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above as though fully set forth herein.

248. The federal Wiretap Act prohibits the interception of any wire, oral, or electronic communications without the consent of at least one authorized party to the communication. See 18 U.S.C. § 2511.

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

250. The Wiretap Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

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

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

253. The Wiretap Act defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo optical system that affects interstate or foreign commerce . . . ." 18 U.S.C. § 2510(12).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

254. Plaintiffs, Defendant, and Tracking Entities are "persons" within the meaning of the Wiretap Act.

255. The Meta Pixel and other Tracking Tools constitute "device[s] or apparatus[es] which can be used to intercept a wire, oral, or electronic communication." 18 U.S.C. § 2510(5).

256. The confidential communications Plaintiffs had with the Website, in the form of, *inter alia*, their search terms and browsing history, were surreptitiously intercepted by the Tracking Entities and such communications were "electronic communications" under 18 U.S.C. § 2510(12).

257. Plaintiffs, like all Users, had a reasonable expectation of privacy in their electronic communications with Defendant's Website, including their Sensitive Information.

258. A reasonable expectation of privacy depends on the nature of the intercepted content. Communications reflecting Users' choices, intent, and behavior on commercial websites, such as searches, browsing, and order interactions, i.e., Sensitive Information, are sensitive and convey the substance and meaning of the communication.

259. The expectation of privacy analysis must begin with reasonable Users assuming that any contents of their communications that were disclosed were disclosed lawfully and with consent. Otherwise, it would create the inference that reasonable Users should expect their privacy to be illegally violated.

260. Moreover, Plaintiffs' electronic communications with the Website included the transmission of their Personal Video Information, which is more sensitive than general electronic communications and browsing information and is afforded greater protection from unauthorized interception, disclosure, and/or transmission.

261. Plaintiffs reasonably expected that Tracking Tools were not intercepting, recording, or disclosing their electronic communications with the Website to the Tracking Entities.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

262. Within the relevant time period, the electronic communications between Plaintiffs and the Website were intercepted by the Tracking Tools the instant they were sent to the Website, without consent, and for the unlawful and wrongful purpose of monetizing their Sensitive Information, which includes the purpose of using such private information to develop advertising and marketing strategies.

263. Interception of Plaintiffs' confidential communications with the Website occurred when Plaintiffs navigated various webpages of the Website.

264. At all times relevant to this complaint, Defendant's conduct was knowing, willful, and intentional, as Defendant is a sophisticated party with full knowledge regarding the functionality of the Tracking Tools. Specifically, Defendant knew that by allowing the Tracking Tools to be implemented on the Website, the Sensitive Information of its Users would be shared with Tracking Entities.

265. Plaintiffs did not consent to the exposure of their confidential electronic communications with the Website to the Tracking Entities. Indeed, such consent could not have been given as Defendant did not seek any form of consent from Plaintiffs for the Tracking Tools' interception, recording, and disclosure of Plaintiffs' Sensitive Information.

266. As detailed above, the Tracking Entities' unauthorized interception and use of Plaintiffs' confidential communications were only possible through Defendant's knowing, willful, or intentional placement of the Tracking Tools on the Website. See 18 U.S.C. § 2511(1)(a).

267. Plaintiffs have been damaged due to the unauthorized interception, disclosure, and use of their confidential communications in violation of 18 U.S.C. § 2520. As such, Plaintiffs are entitled to: (1) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiffs and any profits made by the tracking entities as a result of the violation, or (b) statutory damages of whichever is the greater



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

of $100 per day per violation or $10,000; (2) appropriate equitable or declaratory relief; and (3) reasonable attorneys' fees and other costs reasonably incurred in accordance with the Terms.

**COUNT IV**
**VIOLATIONS OF THE CALIFORNIA INVASION OF PRIVACY ACT**
**Cal. Penal Code § 631**
**(On Behalf of Plaintiffs Roth and Rose and the California Subclass)**

268. Plaintiffs Roth and Rose incorporate by reference and re-allege each and every allegation set forth above as though fully set forth herein.

269. Plaintiffs Roth and Rose bring this count on behalf of themselves and the California Subclass.

270. CIPA provides that a person is liable to another where, "by means of any machine, instrument, contrivance, or in any other manner," committed any of the following: (i) intentionally tapped, or made any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, cable, or instrument of any internal telephonic communication system; or (ii) willfully and without consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state; or (iii) uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained; or (iv) aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit or cause to be done any of the acts or things mentioned above in this section. Cal. Penal Code § 631(a).

271. The Ninth Circuit has confirmed that one of the purposes of wiretapping statutes is to "prevent the acquisition of the contents of a message by an unauthorized third-party . . . ." *In re Facebook Internet Tracking Litig.*, 956 F.3d at 608.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

272. In dealing specifically with CIPA, the California Supreme Court has similarly concluded that the objective of CIPA is to protect a person's communications "from a situation where the other person on the other end of the line permits an outsider" to monitor the communication. *Ribas v. Clark*, 38 Cal. 3d 355, 364 (1985); *see also Smith v. LoanMe*, 11 Cal. 5th 183, 200 (2021).

273. The Website, including the Tracking Tools placed upon it, is a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct at issue here.

274. Within the relevant time period, Plaintiffs Roth and Rose and the California Subclass Members communicated their Sensitive Information to Defendant.

275. Within the relevant time period, Defendant, without the consent of all parties to the communication, or in any unauthorized manner, willfully read or attempted to read or learn the contents or meaning of electronic communications of Plaintiffs and the California Subclass Members, contemporaneous with the communications transit through or passing over any wire, line or cable or with the communications sending from or being received at any place within California.

276. The information collected by the Tracking Tools was not for the sole benefit of Defendant. Within the relevant time period, Defendant aided, agreed with, conspired with, and employed the Tracking Entities to implement the Tracking Tools and to violate Cal. Penal Code § 631.

277. Within the relevant time period, Defendant aided, agreed with, conspired with, and employed the Tracking Entities to implement the Tracking Tools and to violate CIPA § 631.

278. Within the relevant time period, Defendant aided, agreed with, conspired with, and employed the Tracking Entities to accomplish the wrongful conduct at issue here.

279. Plaintiffs Roth and Rose and the California Subclass Members did not authorize or consent to the tracking, interception, and collection of any of their electronic communications.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

280. Plaintiffs Roth and Rose and the California Subclass Members did not authorize or consent to the tracking, interception, and collection of any of their electronic communications. Defendant's violations of Cal. Penal Code § 631 constitutes invasions of privacy of Plaintiffs' and the California Subclass Members' respective rights to privacy.

**COUNT V**
**VIOLATIONS OF THE CALIFORNIA INVASION OF PRIVACY ACT**
**Cal. Penal Code § 638.51**
**(On Behalf of Plaintiffs Roth and Rose and the California Subclass)**

281. Plaintiffs Roth and Rose incorporate by reference and re-allege each and every allegation set forth above as though fully set forth herein.

282. Plaintiffs Roth and Rose bring this count on behalf of themselves and all California Subclass Members.

283. California's Pen Register and Trap and Trace Law is part of CIPA, codified at Cal. Penal Code §§ 630.50-638.55.

284. Pursuant to Cal. Penal Code § 638.51, a person "may not install or use a pen register or a trap and trace device without first obtaining a court order . . . ."

285. A "pen register" is "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

286. A "trap and trace device" is "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." Cal. Penal Code § 638.50(c).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

287. "Process" includes "software that identifies consumers, gathers data, and correlates that data through unique 'fingerprinting.'" *Greenley v. Kochava, Inc.*, 684 F. Supp. 3d 1024, 1050 (S.D. Cal. 2023).

288. Cal. Penal Code § 638.51(a) provides that "a person may not install or use a pen register or a trap and trace device without first obtaining a court order . . . ."

289. No court order to install pen register or trap and trace devices via the Tracking Tools was obtained by Defendant. Defendant uses pen register and trap and trace processes on its Website by deploying Tracking Tools designed to capture phone numbers, email addresses, routing information, addresses, and other signaling information of Website Users. The Tracking Tools identify the source of the incoming electronic and wire communications to the Websites.

290. Defendant's Tracking Tools constitute pen registers and/or trap and trace devices because they are devices or processes that capture incoming electronic or other impulses that identify addressing or signaling information from the electronic communications transmitted by Plaintiffs' and the California Subclass Members' PCs.

291. Defendant did not obtain consent from Plaintiffs Roth and Rose, or the California Subclass Members, before using pen register or trap and trace technology to identify users of its Websites, and has therefore violated Cal. Penal Code § 638.51.

292. As a direct and proximate result of Defendant's conduct, Plaintiffs Roth and Rose and the California Subclass Members suffered losses and were damaged in an amount to be determined at trial. CIPA imposes civil liability and statutory penalties for violations of Cal. Penal Code § 638.51.

## COUNT VI
## VIOLATIONS OF THE CALIFORNIA UNFAIR COMPETITION LAW
## Cal. Bus. & Prof. Code § 17200, et seq.
## (On Behalf of Plaintiffs Roth and Rose and the California Subclass)

293. Plaintiffs Roth and Rose incorporate by reference and re-allege each and every allegation set forth above as though fully set forth herein.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

294. Plaintiffs Roth and Rose bring this count on behalf of themselves and all California Subclass Members.

295. The UCL broadly prohibits acts of "unfair competition," including any "unlawful, unfair or fraudulent business act or practice." See Cal. Bus. & Prof. Code § 17200.

296. Defendant has violated the unlawful prong of the UCL by way of Defendant's above-described violations of the Wiretap Act and CIPA arising from Defendant's purposeful installation and utilization of the Tracking Tools on the Website.

297. Defendant failed to adequately disclose the presence of the Tracking Tools on the Website, which intercepted and transmitted Plaintiffs Roth and Rose's and the California Subclass Members' Sensitive Information to the Tracking Entities without prior knowledge or consent. Defendant facilitated and/or enabled the interception and transmittal of Plaintiffs Roth and Rose's and the California Subclass Members' Sensitive Information to the Tracking Entities to build personal profiles without their knowledge or consent in order to generate additional revenue. Through this conduct, Defendant violated the unfair prong of the UCL.

298. Plaintiffs Roth and Rose have standing to bring claims against Defendant under the UCL. Plaintiffs Roth and Rose's information was tracked and recorded without their consent. Plaintiffs Roth and Rose's data was used to build personal profiles for advertising purposes without consent.

299. Plaintiffs Roth and Rose would have considered it important to their decisions to visit Defendant's Website to know that their data was being tracked and recorded without their consent.

300. Because of Defendant's UCL violations described above, Plaintiffs Roth and Rose suffered injury by losing control of their personal data and having their Sensitive Information tracked and recorded without their consent.

301. Plaintiffs Roth and Rose and the California Subclass Members seek all available relief, including injunctive relief, for Defendant's use of unfair acts or practices.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

**COUNT VII**
**VIOLATIONS OF THE CALIFORNIA CONSTITUTION, Art. 1, § 1**
**(On Behalf of Plaintiffs Roth and Rose and the California Subclass)**

302. Plaintiffs Roth and Rose incorporate by reference and re-allege each and every allegation set forth above as though fully set forth herein.

303. Plaintiffs Roth and Rose bring this count on behalf of themselves and all California Subclass Members.

304. Article I, Section 1 of the California Constitution provides: "[a]ll people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." California Constitution, Article I, Section 1.

305. California voters added the word "and privacy" to the California Constitution when they passed Proposition 11 in 1972. Proposition 11 is also known as the "Privacy Initiative" or "Right to Privacy Initiative."

306. In support of Proposition 11, voters stated that:

> The right of privacy is the right to be left alone … It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulation of personal information. This is essential to social relationships and personal freedom.

307. Plaintiffs Roth and Rose, and the California Subclass Members, have a legally protected interest in their Sensitive Information, such as browsing activity, device identifiers, and related metadata, which Defendant violated by providing the Tracking Entities with access to that data, enabling the interception of such communications. Plaintiffs Roth and Rose, and the California Subclass Members' protected interests arise from various statutes and common law, including, inter alia, the Wiretap Act, the CIPA, and the California Constitution, which protect privacy rights and include the "ability to control circulation of our personal information."



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

308. The privacy rights of Plaintiffs Roth and Rose and the California Subclass Members were invaded through the interception and collection of their data, which included their Sensitive Information and other sensitive information, without first obtaining authorization or consent from Plaintiffs Roth and Rose and the California Subclass Members.

309. Plaintiffs Roth and Rose and the California Subclass Members had a reasonable expectation of privacy when communicating with Defendant's Website and thereby providing and/or transmitting their Sensitive Information.

310. By causing third-party cookies and Tracking Entities to be placed on Users' browsers and devices and by transmitting Users' Sensitive Information to Tracking Entities without consent, Defendant violated their reasonable expectation of privacy.

311. Defendant's intrusion, placing third-party Tracking Tools and enabling third-party access to Users' Sensitive Information without their consent, is and would be highly offensive to a reasonable person.

312. As a direct and proximate result of Defendant's intentional invasion of their privacy rights, Plaintiffs Roth and Rose and the California Subclass Members have been harmed and are entitled to compensatory, punitive, and injunctive relief.

## COUNT VIII
## VIOLATIONS OF THE FLORIDA SECURITY OF COMMUNICATIONS ACT
## Fla. Stat. § 934.01, et seq.
## (On Behalf of Plaintiff Fonseca and the Florida Subclass)

313. Plaintiff Fonseca incorporates by reference and re-alleges each and every allegation set forth above as though fully set forth herein.

314. Plaintiff Fonseca brings this cause of action on behalf of himself and all Florida Subclass Members.

315. The FSCA begins with legislative findings, stating that "[o]n the basis of its own investigations and of published studies, the Legislature makes the following findings...(4) to safeguard the privacy of innocent persons, the interception of wire or oral communications when



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

none of the parties to the communications has consented to the interceptions should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court." Fla. Stat. § 934.01(4).

316. Fla. Stat. § 934.10(1) provides that:

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

317. The FCSA defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in party by a wire, radio, electromagnetic, photoelectronic, or photo-optical systems that affects intrastate, interstate, or foreign commerce." Fla. Stat. § 934.02(12). The FSCA further defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." Fla. Stat. § 934.02(3).

318. The FSCA determines the location of the interception of a communication based on ". . . where the communication originates [from]." *State v. Mozo*, 655 So. 2d 1115, 1117 (Fla. 1995).

319. Fla. Stat. § 934.03(1)(a) prohibits any person from intentionally intercepting, endeavoring to intercept, or procuring any other person to intercept any wire, oral, or electronic communication, except as otherwise specifically provided by statute.

320. Fla. Stat. § 934.03(1)(c) further prohibits any person from intentionally disclosing, or endeavoring to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through an unlawful interception.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

321. Fla. Stat. § 934.03(1)(d) further prohibits any person from intentionally using, or endeavoring to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through an unlawful interception.

322. Defendant's conduct constitutes violations of Fla. Stat. § 934.03(1), where the Website facilitated the Tracking Tools' interception, disclosure, and use of Plaintiff Fonseca's and the Florida Subclass Members' electronic communications without their consent.

323. Fla. Stat. § 934.03(2)(d) provides that interception is unlawful where all parties to the communication have not given prior consent to such interception.[136]

324. Plaintiff Fonseca and the Florida Subclass Members had a reasonable expectation of privacy in their electronic communications with Defendant's Website. Defendant violated Plaintiff Fonseca's and the Florida Subclass Members' reasonable expectation of privacy by intentionally causing the Tracking Tools to be embedded and executed on the Website in a manner that recorded and transmitted the contents of Plaintiff Fonseca's and the Florida Subclass Members' electronic communications to the Tracking Entities contemporaneously with the communications and without Users' knowledge or consent. The transmissions occurred contemporaneously with the communications.

325. Defendant willingly facilitated the interception and collection of Plaintiff Fonseca's and the Florida Subclass Members' communications by embedding and enabling the Tracking Tools on their Website and configuring those tools to transmit data to third-party servers in real time.

326. Defendant used the following items as devices or apparatuses to intercept wire, electronic, or oral communications made by Plaintiff Fonseca and the Florida Subclass Members:

[136] With respect to the FSCA's requirement for prior consent of all parties to the intercepted communication, Fla. Stat. § 934.03(2) contains exceptions related to ministerial operations of employees of communications service providers, criminal investigations by law enforcement, and/or employees of fire stations, public utilities, and ambulance services. None of the aforementioned enumerated exceptions are relevant to Plaintiff Fonseca's claims here.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

a. The Website's source code, which contained Tracking Tools that recorded and disseminated the contents of users' communications as they interacted with the Website;

b. Plaintiff Fonseca's and the Florida Subclass Members' web browsers, which were caused by the Website's code to transmit communications to Tracking Entities;

c. Plaintiff Fonseca's and the Florida Subclass Members' computing and mobile devices;

d. Third-Party Web and advertising servers, which received and processed intercepted communications for the Tracking Entities; and

e. Server-to-server communications between Defendant and the Tracking Entities that enabled the dissemination of users' communications independent of user-initiated disclosures.

327. At all relevant times, Defendant procured the service of, aided, employed, agreed with, and conspired with Tracking Entities to intercept Plaintiff Fonseca's and the Florida Subclass Members' electronic communications while they accessed and interacted with Defendant's Website.

## COUNT IX
## UNJUST ENRICHMENT
## (On Behalf of Plaintiffs and the Class)

328. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above as though fully set forth herein.

329. Plaintiffs bring this cause of action on behalf of themselves and all Class Members.

330. Defendant obtained a benefit by collecting, processing, and enabling third-party monetization of Plaintiffs' and the Class Members' Sensitive Information, which Defendant then used to increase the effectiveness of advertising, marketing, and sales and to generate revenue.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

331. Defendant retained those benefits under circumstances in which the information was collected and transmitted without valid consent. The information was collected and transmitted in breach of Defendant's representations to visitors. Defendant's retention of those benefits is unjust.

332. Plaintiffs and the Class Members conferred these benefits on Defendant, and Defendant has been unjustly enriched at the expense of Plaintiffs and the Class Members. Equity and good conscience require restitution or disgorgement of the benefits unjustly retained by Defendant. Therefore, Plaintiffs and the Class Members are entitled to the relief set forth below.

## PRAYER FOR RELIEF

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

a. For an order determining that this action is properly brought as a class action and certifying Plaintiffs as the representatives of the Class and their counsel as Class Counsel;

b. For an order declaring the Defendant's conduct violates the statutes referenced herein;

c. For an order finding in favor of Plaintiffs, the Class, and Subclasses on all counts asserted herein;

d. Entry of an order for injunctive and declaratory relief as described herein, including, but not limited to, requiring Defendant to immediately (i) remove the Tracking Tools from the Website or (ii) add, and obtain, the appropriate consent from Users;

e. For damages in amounts to be determined by the Court and/or jury;

f. An award of statutory damages or penalties to the extent available;

g. For pre-judgment interest on all amounts awarded;

h. For an order of restitution and all other forms of monetary relief;



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

i. An award of all reasonable attorneys' fees and costs; and

Such other and further relief as the Court deems necessary and appropriate.

**DEMAND FOR TRIAL BY JURY**

Plaintiffs hereby demand a trial by jury.

DATED this 29th day of April, 2026.

TOUSLEY BRAIN STEPHENS PLLC

By: *Kim D. Stephens, P.S.*
By: *Rebecca L. Solomon*

Kim D. Stephens, P.S., WSBA #11984
kstephens@tousley.com
Rebecca L. Solomon, WSBA #51520
rsolomon@tousley.com
1200 Fifth Avenue, Suite 1700
Seattle, Washington, 98101
Telephone: 206.682.5600/Fax: 206.682.2992

Mark S. Reich*
mreich@zlk.com
LEVI & KORSINSKY, LLP
33 Whitehall Street, 27th Floor
New York, NY 10004
Telephone: 212.363.7500/Fax: 212.363.7171

**pro hac vice* forthcoming

***Attorneys for Plaintiffs and Putative Class***



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992