

KOPELOWITZ OSTROW P.A.
Kristen Lake Cardoso (SBN 338762)
cardoso@kolawyers.com
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Telephone: 954-525-4100

Attorney for the Plaintiff and the Proposed Classes

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION**

Case No.

ARSHAM KOSARI, *on behalf of himself and
all others similarly situated,*

Plaintiff,

v.

META PLATFORMS, INC., SAMASOURCE
IMPACT SOURCING INC., d/b/a SAMA, and
LUXOTTICA OF AMERICA, INC.

Defendants.

CLASS ACTION COMPLAINT AND
DEMAND FOR JURY TRIAL

Plaintiff Arsham Kosari (“Plaintiff”) brings this class action complaint (“Complaint”) on behalf of himself and all others similarly situated (“Class Members”) against Defendant Meta Platforms, Inc. (“Meta”), Defendant Samasource Impact Sourcing, Inc., d/b/a Sama (“Sama”), and Defendant Luxottica of America, Inc. (“Luxottica”)(collectively, “Defendants”) for the privacy violations alleged herein, which are based on Plaintiff’s knowledge of facts pertaining to himself and his own actions and counsel’s investigations, and upon information and belief as to all other matters, are as follows:

I. NATURE OF THE CASE

1. This case arises out of the inappropriate use of Plaintiff’s and Class Members’ private recordings on their Meta AI Glasses and specifically, Meta unlawfully sharing the audio and visual recordings to enhance and train its large language models.

2. Meta continues to misrepresent its products and services, and its AI-enabled smart glasses, which are marketed under the Ray-Ban and Oakley brands (collectively, the “Meta AI Glasses” or “Glasses”), are the latest in a multi-decade pattern of bad conduct that, by design, invades the lives of ordinary citizens and bystanders.

3. Meta designs, controls, and operates the AI software, cloud infrastructure, and data pipelines embedded in these Glasses.

4. Sama is Meta's subcontractor responsible for the human review and annotation of video, audio, and image data captured by the Meta AI Glasses.

5. Meta transmits footage captured through the Glasses—including highly intimate recordings of users in their homes, bedrooms, and bathrooms—to Sama's data annotation facilities in Nairobi, Kenya, where thousands of human workers manually view, label, and assess that footage to train Meta's artificial intelligence models.

6. Meta markets its AI Glasses as an “all-in-one assistant” that empowers wearers to “remain in control of their privacy.”¹ The opposite is true.

7. When a user activates the Glasses by pressing a physical button or uttering the wake phrase “Hey Meta,” the device captures high-resolution video and audio and transmits that data through the user's smartphone to Meta's cloud servers and Sama’s processing center.²

8. From there, Meta routes selected footage into a data annotation pipeline managed by Sama, where low-wage contractors in Nairobi sit in rows of cubicles, drawing bounding boxes around objects, labeling images, checking transcriptions, and performing quality assurance all while viewing, in full resolution, the most private moments of unsuspecting Americans' lives.

9. The content these workers see is staggering. Multiple Sama employees were interviewed by Swedish investigative journalists and described footage of people using bathrooms,

¹ Naipano Lepapa et al., *She Came Out of the Bathroom Naked, Employee Says*, Svenska Dagbladet (Feb. 27, 2026).

² Meta, *Supplemental Meta Platforms Technologies Privacy Policy* (Oct. 21, 2025).

undressing, engaging in sexual activity, and inadvertently exposing bank card details and other financial information.³

10. One worker recounted: “I saw a video where a man puts the glasses on the bedside table and leaves the room. Shortly afterwards his wife comes in and changes her clothes.”⁴ Another stated: “*We see everything—from living rooms to naked bodies*. Meta has that type of content in its databases.”⁵ A third described sex scenes filmed with the Glasses: “*someone is wearing them having sex. That is why this is so extremely sensitive*.”⁶

11. Plaintiff brings this class action on behalf of a Nationwide Class and a Florida Subclass and seeks compensatory, statutory, and punitive damages, disgorgement, and injunctive and declaratory relief for Meta's violations of (1) the Electronic Communications Privacy Act (“ECPA”), 18 U.S.C. §§ 2510–2522; (2) the Florida Security of Communications Act (“FSCA”), Fla. Stat. §§ 934.01–934.50; (3) Invasion of Privacy; and (4) Unjust Enrichment.

II. THE PARTIES

A. Plaintiff

12. Plaintiff is a citizen and resident of Broward County, Florida, and has resided in Florida at all times relevant to this Complaint. In or around April 2025 Plaintiff received the Ray-Ban Meta Skyler (Gen 1) as a gift.

13. Plaintiff desired and obtained the Meta AI Glasses in reliance on Meta's widespread marketing and advertising campaign, including representations that the glasses were “designed for privacy,” “controlled by you,” and “built for your privacy and others too.”

14. Plaintiff used the Meta AI Glasses' voice-activated AI assistant feature by speaking the wake phrase “Hey Meta” to ask questions, identify objects, and utilize other AI-powered features advertised by Meta.

³ Lepapa et al., *She Came Out of the Bathroom Naked*, Svenska Dagbladet (Feb. 27, 2026).

⁴ *Id.*

⁵ *Id.*

⁶ *Id.*

1 15. When Plaintiff used these AI features, the Meta AI Glasses captured video and
2 audio of Plaintiff's surroundings and transmitted this content to Meta's servers in real time.

3 16. On numerous occasions, Plaintiff used the Meta AI Glasses while in his home,
4 including in private spaces where he had a reasonable expectation of privacy.

5 17. Plaintiff was not informed, and did not consent to, Meta routing his captured video
6 and audio footage to third-party human contractors employed by Sama in Nairobi, Kenya, for
7 manual review, annotation, and use in training Meta's AI models.

8 18. Plaintiff is experiencing feelings of anxiety, stress, fear, and frustration as a result
9 of the invasion of his privacy. This goes far beyond allegations of mere worry or inconvenience;
10 it is exactly the sort of injury and harm to a victim that the law contemplates and addresses.

11 19. Plaintiff does not recall Meta disclosing any disclaimers or explicit warnings about
12 its intent to copy and share his private audio and visual recordings.

13 20. Plaintiff has suffered harm including invasion of privacy, loss of the benefit of his
14 bargain, and statutory damages as set forth herein.

15 **B. Defendants**

16 21. Defendant **Meta Platforms, Inc.** is a Delaware corporation with its principal place
17 of business at 1 Meta Way, Menlo Park, California 94025. Meta designs, manufactures (in
18 partnership with EssilorLuxottica S.A.), distributes, markets, and sells the Meta AI Glasses. Meta
19 owns and operates the AI software, cloud infrastructure, data processing systems, and contractual
20 relationships through which user-captured footage flows from the Glasses to Meta's servers and
21 onward to its subcontractors. Meta controls the data pipeline at every stage: from the on-device
22 wake-word detection system, to the smartphone app that serves as the connectivity intermediary,
23 to the cloud servers that receive and store the footage, to the annotation queues that route footage
24 to human reviewers, to the AI models that consume the resulting labeled data. Meta generated over
25 \$200 billion in revenue in fiscal year 2025.⁷

26
27 ⁷ See, e.g., *Meta's AI Transformation: Analyzing the Llama Integration and the \$200 Billion Ad-*
28 *Tech Engine*, FinTerra (Jan. 27, 2026).

22. Defendant **Samasource Impact Sourcing, Inc.**, d/b/a **Sama**, is a Delaware corporation with its principal offices at 2017 Mission Street, Suite 301, San Francisco, California 94110. Sama operates data annotation facilities on Mombasa Road in Nairobi, Kenya, where it employs thousands of data annotators who manually review, label, and annotate video, audio, and image data for Meta and other technology clients. Sama workers assigned to Meta's AI Glasses project review footage captured by the Glasses' cameras—including intimate footage of users and individuals in their vicinity—to train Meta's AI models. Sama operates under Meta's direction and control, executing annotation tasks according to Meta's specifications, within an intensely monitored work environment that bans personal smartphones and surveils the workforce with cameras.

23. **Defendant Luxottica of America, Inc.** is an Ohio corporation with its principal place of business located at 4000 Luxottica Place, Mason, OH 45040-8114. On information and belief, Luxottica of America, Inc., in partnership with Meta, advertises, markets, and sells the Meta AI Glasses throughout the United States. The unfair, unlawful, deceptive, and misleading Challenged Representations and Omissions on the Products were prepared, authorized, ratified, and/or approved by Luxottica and its agents, and were disseminated throughout California and the nation by Luxottica and its agents to deceive and mislead consumers in the State of California and throughout the United States into purchasing the Meta AI Glasses.

III. FACTUAL ALLEGATIONS

A. Meta's Transition from Social Media Platform to AI Competitor

24. Meta produces the Meta AI Glasses in partnership with EssilorLuxottica S.A., the French-Italian eyewear conglomerate that owns the Ray-Ban and Oakley brands. The current product lineup includes: the Ray-Ban Meta (first and second generation), the Oakley Meta HSTN, the Oakley Meta Vanguard, and the Meta Ray-Ban Display.⁸

⁸ See Uploadvr.com, *Meta & EssilorLuxottica Sold 7 Million Smart Glasses in 2025* (Feb. 11, 2026).

1 25. The Glasses are powered by a Qualcomm Snapdragon AR1 Gen1 system-on-chip
2 and feature integrated 12-megapixel cameras capable of capturing both still photographs and high-
3 definition video, a multi-microphone array for voice capture and ambient audio recording, open-
4 ear speakers, and Bluetooth and Wi-Fi connectivity for data transmission.

5 26. The Glasses operate in two recording modes. First, users can manually capture
6 photos and video by pressing a physical button on the right temple of the frame. Second, users can
7 activate Meta's AI assistant by speaking the wake phrase “Hey Meta,” which triggers the Glasses
8 to begin recording audio and, in many modes, video, and to transmit that data to Meta's cloud
9 servers for AI processing.

10 27. Meta markets the Glasses as a revolutionary personal assistant. At Meta Connect
11 in September 2025, CEO Mark Zuckerberg personally demonstrated the Glasses, preaching that
12 they would serve as an “all-in-one assistant” offering live translation, visual recognition, travel
13 guidance, and real-time information.⁹ Meta touts the Glasses as a device that lets users “remain in
14 control of their privacy.”¹⁰

15 28. That representation is false. As described herein, Meta designed the Glasses to
16 capture intimate audiovisual data, transmit it to remote servers, and route it to overseas contractors
17 for human review—while burying the scope of this data collection across a thicket of fragmented,
18 misleading, and contradictory privacy policies.

19 29. The Glasses have achieved explosive commercial success. EssilorLuxottica
20 reported in its Q4 2025 earnings that it sold over seven million AI-enabled smart glasses in 2025
21 alone—more than tripling the two million units sold in 2023 and 2024 combined.¹¹ Based on
22 EssilorLuxottica's reported North American revenue share of approximately 46%, an estimated 3.2
23 million of these units were sold in the United States. The companies are now discussing plans to
24 increase annual production capacity to 20–30 million units.

25 _____
26 ⁹ Lepapa et al., *She Came Out of the Bathroom Naked*, Svenska Dagbladet (Feb. 27, 2026).

27 ¹⁰ *Id.*

28 ¹¹ CNBC, *Ray-Ban Maker EssilorLuxottica Triples Sales of Meta AI Glasses* (Feb. 11, 2026).

30. Meta's AI Glasses are not an isolated product—they are a central pillar of Meta's corporate transformation from a social media platform into an AI infrastructure company. Meta has staked its future on artificial intelligence, and the Glasses are the hardware vehicle through which Meta intends to embed its AI into the physical world.

31. Meta spent approximately \$38–40 billion on capital expenditures in 2024 and raised its 2025 capital expenditure outlook to \$64–72 billion, directed primarily at AI infrastructure, including data centers, GPU clusters, and model training.¹² Meta projects capital expenditures nearing \$100 billion in 2026.¹³

32. Meta's AI strategy centers on its proprietary Llama series of large language models (“LLMs”). Meta released Llama 2 in 2023, Llama 3 in 2024, and Llama 4 in early 2025.¹⁴ Llama 4 provides the backbone for Meta AI, the AI assistant integrated into WhatsApp, Instagram, and—critically—the Meta AI Glasses. Meta AI reached over one billion monthly active users.¹⁵

33. The AI Glasses are uniquely important to Meta's strategy because they are the only Meta product that captures real-world audiovisual data from the physical environment. Unlike Facebook or Instagram—which receive data that users voluntarily upload—the Glasses passively capture the world around the wearer: their home, their family, their conversations, their most private moments. This captured data is the raw material Meta needs to train its multimodal AI models to understand and interpret the physical world. On the Q2 2025 earnings call, Zuckerberg stated: “I think AI glasses are gonna be the main way that we integrate superintelligence into our day-to-day lives.”¹⁶

¹² See Constellationr.com, *Meta Ups Its 2025 Spending on AI, Data Centers* (Apr. 30, 2025).

¹³ FinTerra, *Analyzing the Llama Integration and the \$200 Billion Ad-Tech Engine* (Jan. 27, 2026).

¹⁴ See Yahoo Finance, *Why Meta Platforms' Open-Source AI Strategy Might Win the Long Game* (Oct. 17, 2025).

¹⁵ Gizmodo, *Meta's New Privacy Policy Opens Up AI Chats for Targeted Ads* (Jan. 1, 2026).

¹⁶ <https://www.bloomberg.com/news/articles/2026-01-13/meta-said-to-discuss-doubling-ray-ban-glasses-output-after-surge-in-demand> (last visited Mar. 9, 2026).

34. Meta has constructed an AI ecosystem in which the Glasses are the sensory input, the Llama models are the processing engine, and Meta's advertising platform, which reached a \$60 billion annual run rate through its AI-driven Advantage+ system in 2025, is the monetization output.¹⁷ The data captured from users through the Glasses feeds directly into this monetization model: better training data produces smarter models, smarter models produce better ad targeting, and better ad targeting produces more revenue.

35. Meta's entire AI architecture depends on a continuous supply of real-world audiovisual training data—data that is extracted from millions of users under a framework designed to maximize collection while minimizing transparency.

B. Meta's Glasses Intercept, Transmit, Record, and Divulge Highly Sensitive Data Without Users' (or Bystanders) Knowledge or Consent

36. When a user activates the AI function on the Meta AI Glasses, whether by pressing the capture button or speaking “Hey Meta,” the Glasses capture audio and video data and transmit it via Bluetooth (or Wi-Fi when available) to the user's paired smartphone running the Meta AI app. The smartphone performs intermediate processing (including HDR rendering and image stabilization) and then transmits the data to Meta's cloud servers.

37. Meta operates approximately 24 data center campuses globally, with at least 18 operational facilities in the United States, and additional facilities in the EU. Testing by Swedish investigative journalists confirmed consistent data transmissions from the Glasses to Meta servers during normal operation.

38. When users ask Meta AI questions about what they see, the Glasses transmit data to Meta's cloud for AI processing, which is then used to improve Meta products and train its AI.

39. However, Meta does not disclose which cloud infrastructure receives this data, where data reviewers are located, or that its data reviewers are actually underpaid data annotators employed by a commercial subcontractor on another continent, 7,000 miles away.

¹⁷ FinTerra, *Analyzing the Llama Integration and the \$200 Billion Ad-Tech Engine* (Jan. 27, 2026).

40. From Meta's servers, selected footage enters a data annotation pipeline managed by Sama in Nairobi, Kenya. The onward transfer of user data from Meta's U.S. servers to Sama's Nairobi annotation queues is the legally operative data flow for the claims alleged herein—a cross-border transfer confirmed by contractor testimony and the Swedish investigation.

41. On February 27, 2026, Swedish newspapers Svenska Dagbladet and Göteborgs-Posten published a joint investigation, titled “Your Eyes, Their Data” (Swedish: *Dina ögon, deras data*), based on interviews with more than thirty employees at different levels of Sama's Nairobi operations. The investigation was conducted in collaboration with Naipanoi Lepapa, an award-winning investigative freelance journalist based in Nairobi.

42. The reporters met Sama workers at a hotel in Nairobi, at a safe distance from Sama's offices on Mombasa Road. Some workers arrived straight from night shifts; others were preparing for ten-hour shifts. All spoke on condition of anonymity because they had signed extensive confidentiality agreements and feared termination—and with it, a return to poverty.

43. The workers described what they see on their screens every day. Multiple Sama employees working specifically on annotating videos, images, and speech for Meta's AI systems reported seeing footage of:

- **Bathroom visits:** People using toilets and bathing, captured by Glasses left in bathrooms or worn by household members;
- **Nudity:** Individuals undressing, captured unknowingly—for example, a man placed his Glasses on a bedside table, and the still-recording device captured his wife entering the room and changing clothes;
- **Sexual activity:** Sex scenes filmed by users wearing the Glasses during intercourse;
- **Financial information:** Bank cards, credit cards, and other sensitive financial documents visible on screen; and
- **Private conversations:** Text transcriptions of “any topics at all,” including discussions of crimes, protests, and sexually explicit descriptions of other people.¹⁸

¹⁸ Lepapa et al., *She Came Out of the Bathroom Naked*, Svenska Dagbladet (Feb. 27, 2026).

1 44. One worker stated: “In some videos you can see someone going to the toilet, or
2 getting undressed. I don't think they know, because if they knew they wouldn't be recording.”¹⁹

3 45. Another stated: “We see everything—from living rooms to naked bodies. Meta
4 has that type of content in its databases. People can record themselves in the wrong way and not
5 even know what they are recording. They are real people like you and me.”²⁰ A third described the
6 footage as capable of triggering “enormous scandals” if leaked.²¹

7 46. One worker described the psychological burden: “When you see these videos, it
8 feels that way [like looking into someone's private life]. But since it is a job, you have to do it.
9 You understand that it is someone's private life you are looking at, but at the same time you are
10 just expected to carry out the work. You are not supposed to question it. If you start asking
11 questions, you are gone.”²²

12 47. Meta's purported safeguard for this pipeline—an automatic face-blurring
13 algorithm—does not reliably function. A former Meta employee acknowledged this failure: “The
14 algorithms sometimes miss. Especially in difficult lighting conditions, certain faces and bodies
15 become visible.”²³

16 48. The journalists also purchased their own pair of Meta AI Glasses and tested them.
17 They found that: (a) the AI functions cannot operate solely through local, on-device processing—
18 an internet connection is required; (b) network traffic analysis showed frequent and consistent data
19 transmissions to Meta servers; and (c) the claim made by retail sales staff that “nothing is shared”
20 with Meta and that “everything stays locally in the app” is demonstrably false.²⁴

21
22
23 ¹⁹ *Id.*

24 ²⁰ *Id.*

25 ²¹ *Id.*

26 ²² *Id.*

27 ²³ *Id.*

28 ²⁴ *Id.*

49. Meta was given two months to respond to the journalists' questions about how the company informs users about the Glasses, what filters prevent private material from reaching annotators, how the chain of subcontractors is audited, and why footage showing extremely private situations reaches annotation queues. After two months, Meta's spokesperson in London, Joyce Omope, responded with a letter that did not directly answer any of the questions—instead referring the journalists to Meta's AI terms of use and privacy policy.²⁵

50. When asked to explain how sharing highly private material with subcontractors in Kenya can be reconciled with its privacy policy, Meta and Sama did not respond.²⁶

51. Meta's refusal to address these specific questions, despite extended lead time, underscores that consumers were never provided clear, direct notice of human review of intimate content.

C. Class Members Did Not Consent to Meta's Conduct

i. Meta's Conduct Exceeds Any Purported Consent, and Its Privacy Policies Are Fragmented and Inadequate

52. Meta's privacy disclosure framework for the AI Glasses is spread across no fewer than four separate documents: (1) the Supplemental Meta Platforms Technologies Privacy Policy; (2) the Meta AI Terms of Service; (3) the Meta Voice Controls Privacy Notice; and (4) the Supplemental Meta Platforms Technologies Terms of Service. Each document cross-references the others, creating a labyrinth of disclosures that no reasonable consumer would read in full, let alone synthesize into a coherent understanding of how their data is actually used.

53. This fragmentation is not accidental, it is by design. The critical disclosures about human review are buried in subsections nominally about voice recording storage, separated from the default-on disclosures about transcript storage. A user who reads only the primary privacy policy—which is itself lengthy and densely cross-referenced—would not learn that “trained

²⁵ *Id.*

²⁶ *Id.*

reviewers” means underpaid data annotators employed by a commercial subcontractor in Nairobi, Kenya. Meta never defines “trained reviewers” in any of its policies.

54. Simply put, Meta does not specify what “third parties” means, does not name Sama, does not identify Kenya as a processing location, and it does not describe *human review of intimate video footage*.

55. All of this information is and was highly relevant to Plaintiff and Class Members when they decided to purchase and use the Glasses.

56. At no point in any of Meta's privacy documents does Meta disclose: (a) that intimate video footage—including nudity, sexual activity, and bathroom visits—is reviewed by human annotators; (b) that those annotators are employed by Sama, a commercial data-labeling subcontractor; (c) that the annotation takes place in Nairobi, Kenya; (d) that Meta's face-anonymization algorithm frequently fails, leaving faces and bodies visible to reviewers; or (e) that footage captured during false or accidental activations of the “Hey Meta” wake word also enters the annotation pipeline.

57. No reasonable consumer reading Meta's privacy policies—individually or collectively—would understand that wearing the Glasses in their home could result in footage of their spouse undressing, their child bathing, or their private conversations being transmitted to a warehouse in Kenya and viewed by strangers.

ii. Meta's Framework Fails to Provide a Reasonable Opt-Out

58. On April 29, 2025, Meta fundamentally restructured the default privacy settings for the AI Glasses. Prior to that date, users could choose whether to enable Meta AI with camera functionality and could toggle voice recording storage on or off. After April 29, 2025, Meta enabled Meta AI with camera functionality by default on all Glasses.²⁷ Meta simultaneously removed the option for users to opt out of voice recording storage entirely.

²⁷ TechCrunch <https://techcrunch.com/2025/04/30/if-you-own-ray-ban-meta-glasses-you-should-double-check-your-privacy-settings/> (last visited Mar. 9, 2026).

59. Following the April 2025 change, voice recordings and transcripts are stored by default and may be retained for up to one year. The only mechanism now available to users who wish to avoid retention is to manually delete each individual recording from the app—a per-recording burden that no reasonable consumer would undertake for every AI interaction. Unintended activations (“false wakes”) are supposed to be deleted within 90 days, but even that reduced period means Meta retains recordings of conversations the user never intended to initiate.

60. Meta communicated the April 2025 changes through a generic email to existing users that described the update as a routine privacy policy update. Meta did not use the words “opt-out removed,” “setting discontinued,” or “you must now manually delete” in this email notice.

61. As such, any continued use does not constitute acceptance or consent given that Meta’s unilateral amendment lacks adequate notice of material changes.²⁸

62. For video data captured during Live AI sessions, Users have no way to know how long Meta retains video of their homes, their families, and their most private moments—or when, if ever, that data is deleted.

D. Technical Framework

i. Data Flows from the Glasses to Sama's Annotation Queues

63. The Meta AI Glasses operate on a four-stage data architecture. The Glasses contain an on-device microcontroller for wake-word detection (the “Hey Meta” trigger) and a Qualcomm Snapdragon AR1 Gen1 system-on-chip for audio/video capture. When “Hey Meta” is detected—or the capacitive capture button is pressed—the device begins recording and transmitting data. The audio and video data are transmitted via Bluetooth (or Wi-Fi when available) to the paired smartphone running the Meta AI app and Meta's cloud infrastructure. The data on Meta's servers enters the data annotation pipeline managed by Sama in Nairobi, Kenya. Sama workers manually review the footage: drawing bounding boxes around objects, assigning labels, checking transcriptions, and performing quality assurance. The labeled data is then used to train and refine Meta's AI models.

²⁸ See *Nguyen v. Barnes & Noble, Inc.*, 763 F.3d 1171 (9th Cir. 2014).

64. A single “Hey Meta” invocation in a user's living room results in: (a) on-device audio and video capture; (b) wireless transmission to the paired smartphone and Meta's cloud servers; and (c) potential routing of the footage to a human annotator in Kenya who views, labels, and annotates the content. At no stage does the user receive real-time notice that their footage may be viewed by a human being.

65. The “Hey Meta” wake-word detection system is imprecise, and Meta’s policies define voice interactions to include accidental activations and background sound during interactions.

66. The imprecision of the wake-word system means that the Glasses may begin recording at any time in response to ambient speech—capturing conversations the user never intended to record and never knew were being transmitted to Meta's servers.

ii. Statutory Framework

67. The Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2522, prohibits the intentional interception, disclosure, and use of wire, oral, or electronic communications. 18 U.S.C. § 2511(1). The statute provides a private right of action under 18 U.S.C. § 2520, with statutory damages of the greater of \$100 per day for each day of violation or \$10,000, plus actual damages, profits made by the violator, punitive damages, and reasonable attorneys' fees. 18 U.S.C. § 2520(c)(2).

68. Although the ECPA contains a one-party consent exception—permitting interception where one party to the communication has consented—that exception does not apply “where such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.” 18 U.S.C. § 2511(2)(d). This is known as the “crime-tort exception.”

69. Recent decisions in this District, have held that plaintiffs adequately alleged invasion of privacy sufficient to trigger the ECPA crime-tort exception.

70. Meta's conduct satisfies the crime-tort exception. Meta intercepts users' private communications—including audio, video, and text transmitted through the Glasses to its servers and onward to Sama—for the purpose of committing the independent tort of intrusion upon

1 seclusion. Meta's purpose in intercepting this data is to train its AI models, which Meta
2 accomplishes by routing intimate footage of private moments to human annotators in Kenya. The
3 routing of video showing nudity, sexual activity, bathroom visits, and financial information to
4 overseas contractors for manual viewing—without adequate notice or consent—constitutes an
5 intentional intrusion upon the solitude and seclusion of Plaintiff and Class Members that would be
6 highly offensive to any reasonable person. Because Meta's interception of these communications
7 is undertaken for the purpose of this tortious conduct, the one-party consent exception is
8 inapplicable, and Meta's ECPA liability attaches.

9 71. The Florida Security of Communications Act, Fla. Stat. § 934.03, independently
10 prohibits the intentional interception of wire, oral, or electronic communications without the
11 consent of *all* parties to the communication. Unlike the federal ECPA, Florida is an all-party-
12 consent jurisdiction: no interception is lawful unless every person whose communication is
13 captured has given prior consent. Fla. Stat. § 934.03(2)(d). Moreover, it is independently “unlawful
14 to intercept any wire, oral, or electronic communication for the purpose of committing any criminal
15 act.” Fla. Stat. § 934.03(2)(e).

16 72. The FSCA provides a private right of action under Fla. Stat. § 934.10. Any person
17 whose wire, oral, or electronic communication is intercepted, disclosed, or used in violation of §§
18 934.03–934.09 is entitled to recover: (a) preliminary, equitable, or declaratory relief; (b) actual
19 damages, but not less than liquidated damages computed at the rate of \$100 per day for each day
20 of violation, or \$1,000, whichever is higher; (c) punitive damages; and (d) reasonable attorneys'
21 fees and litigation costs. Fla. Stat. § 934.10(1).

22 73. Meta's conduct violates the FSCA because it intercepts the oral and electronic
23 communications of Florida Class Members—audio and video captured by the Glasses and
24 transmitted to Meta's servers and Sama's annotation queues—without obtaining the consent of all
25 parties to those communications. Florida users who speak in the presence of the Glasses, whose
26 conversations are captured by the “Hey Meta” activation (whether intentional or accidental), and
27 whose footage is transmitted to Meta and Sama, have not consented to interception by Meta's data
28 annotation contractors. The FSCA's all-party-consent requirement demands affirmative consent

from every person whose communication is intercepted—not merely from the wearer who pressed the button or spoke the wake word.

CLASS ACTION ALLEGATIONS

74. Plaintiff brings this action on behalf of himself and all others similarly situated, pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), and 23(b)(3), and seeks certification of the following Classes:

Nationwide Class: All persons residing in the United States who, during the Class Period,²⁹ used Meta AI Glasses and whose audio, video, or electronic communications were intercepted, recorded, transmitted, stored, or disclosed by Meta and/or Sama.

Florida Subclass: All persons residing in the State of Florida who, during the Class Period, used Meta AI Glasses and whose wire, oral, or electronic communications were intercepted, recorded, transmitted, stored, or disclosed by Meta and/or Sama.

75. **Excluded** from the Classes are: (a) Defendants and any entity in which either has a controlling interest; (b) the current and former officers, directors, and employees of Defendants; (c) the judges and court staff assigned to this matter; and (d) counsel for all parties.

76. **Numerosity.** The Classes are so numerous that joinder of all members is impracticable. EssilorLuxottica reported sales of over seven million AI-enabled smart glasses in 2025 alone, with an estimated 3.2 million units sold in the United States.³⁰ The precise size of the Classes is currently unknown to Plaintiff but is readily ascertainable through Meta's own records, which track registered device owners and their geographic locations. Each Class consists of well over a million individuals.

77. **Predominant Common Questions.** The Classes' claims present several questions of law and fact common to all members that predominate over any questions affecting individual Class Members, including:

²⁹ Plaintiff's understanding of Meta's conduct is still evolving. As such, the "Class Period" is the earliest date permitted by law through present.

³⁰ <https://www.cnbc.com/2026/02/11/ray-ban-maker-essilorluxottica-triples-sales-of-meta-ai-glasses.html> (last visited Mar. 9, 2026).

(a) Whether Meta intercepted, recorded, transmitted, stored, or disclosed Class Members' communications through the Meta AI Glasses;

(b) Whether Meta's interception of Class Members' communications was undertaken for the purpose of committing a criminal or tortious act within the meaning of 18 U.S.C. § 2511(2)(d);

(c) Whether Meta's conduct constitutes intrusion upon seclusion;

(d) Whether Meta's privacy policies provided adequate notice of, or obtained valid consent for, the human review of Class Members' footage by Sama contractors;

(e) Whether Meta violated the ECPA, 18 U.S.C. §§ 2510–2522;

(f) Whether Meta and/or Sama violated the FSCA, Fla. Stat. §§ 934.03–934.09;

(g) Whether Meta was unjustly enriched by its interception and use of Class Members' communications; and

(h) Whether Plaintiff and Class Members are entitled to damages, including statutory, compensatory, and punitive damages, disgorgement, and injunctive relief.

78. Typicality. Plaintiff's claims are typical of all Class Members because they arise from the same course of conduct by Defendants and are based on the same legal theories. Plaintiff used the Meta AI Glasses, and Plaintiff's communications were intercepted, transmitted, stored, and disclosed to Sama in the same manner as all Class Members.

79. Adequate Representation. Plaintiff will fairly and adequately represent the Classes and protect the interests of all Class Members. Plaintiff has retained competent counsel with significant experience in class action and data privacy litigation. Plaintiff and counsel have no interests that conflict with the interests of the Classes and are not subject to any unique defenses. Plaintiff and counsel will vigorously prosecute this action to advance the interests of the Classes and have the resources necessary to do so.

80. Superiority. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. Joinder of all Class Members is impracticable. Individual litigation would impose an unreasonable burden on the courts and on the parties, would create a risk of inconsistent or contradictory judgments, and would be inefficient given that the

claims arise from uniform conduct directed at millions of consumers. Class-wide adjudication provides comprehensive oversight by a single court and avoids duplicative proceedings.

81. Plaintiff reserves all rights to revise or modify the class allegations based on facts and legal developments following additional investigation or discovery.

IV. CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION

Violation of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2522 On Behalf of Plaintiff and the Nationwide Class

82. Plaintiff re-alleges and incorporates the paragraphs 1 through 81 above as if fully restated herein.

83. The ECPA prohibits any person from intentionally intercepting, endeavoring to intercept, or procuring any other person to intercept or endeavor to intercept any wire, oral, or electronic communication. 18 U.S.C. § 2511(1)(a).

84. The ECPA 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 the interception of such a communication in violation of the Act. 18 U.S.C. § 2511(1)(c).

85. The ECPA 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 the interception of such a communication in violation of the Act. 18 U.S.C. § 2511(1)(d).

86. Meta intentionally intercepted Plaintiff's and Class Members' wire, oral, and electronic communications by capturing audio and video data through the Meta AI Glasses and transmitting that data to its cloud servers and onward to Sama's annotation facilities in Kenya—without adequate notice or consent.

87. Meta intentionally disclosed the contents of Plaintiff's and Class Members' intercepted communications by transmitting that footage to Sama, a third-party commercial subcontractor, for manual human review and annotation.

1 88. Meta intentionally used the contents of Plaintiff's and Class Members' intercepted
2 communications to train and refine its AI models, enhance its products, and power its advertising
3 platform.

4 89. Although 18 U.S.C. § 2511(2)(d) provides a consent exception where one party to
5 the communication has consented, that exception is inapplicable here because Meta intercepted
6 Plaintiff's and Class Members' communications “for the purpose of committing [a] criminal or
7 tortious act in violation of the Constitution or laws of the United States or of any State.” 18 U.S.C.
8 § 2511(2)(d).

9 90. Specifically, Meta intercepted Plaintiff's and Class Members' communications for
10 the purpose of committing the tort of intrusion upon seclusion, as described in the Fourth Cause
11 of Action below. Meta's interception and onward transmission of intimate footage—including
12 nudity, sexual activity, bathroom visits, and private conversations—to overseas contractors for
13 manual viewing constitutes an intentional intrusion upon the solitude and seclusion of Plaintiff and
14 Class Members that is highly offensive to a reasonable person. Because Meta's purpose in
15 intercepting these communications was to commit this independent tortious act, the one-party
16 consent exception does not shield Meta from ECPA liability.³¹

17 91. Meta's violations of the ECPA are ongoing and continuous. Each day that Meta
18 intercepts, discloses, and uses Plaintiff's and Class Members' communications without lawful
19 consent constitutes a separate violation of the statute.

20 92. Pursuant to 18 U.S.C. § 2520, Plaintiff and the Nationwide Class are entitled to: (a)
21 preliminary, equitable, and declaratory relief; (b) damages, including actual damages and any
22 profits made by Meta as a result of its violations, or statutory damages of the greater of \$100 per
23 day for each day of violation or \$10,000, whichever is greater; (c) punitive damages; and (d)
24 reasonable attorneys' fees and litigation costs.

25 **SECOND CAUSE OF ACTION**

26 **Violation of the Florida Security of Communications Act, Fla. Stat. §§ 934.03–934.10 On Behalf of Plaintiff and the Florida Subclass**

27 ³¹ See *Semien v. PubMatic Inc.*, No. 5:24-cv-05765 (N.D. Cal.); *Krzyzek v. OpenX Techs., Inc.*,
28 No. 5:24-cv-06379 (N.D. Cal.).

1 93. Plaintiff re-alleges and incorporates paragraphs 1 through 81 above as if fully
2 restated herein.

3 94. The FSCA prohibits any person from intentionally intercepting, endeavoring to
4 intercept, or procuring any other person to intercept or endeavor to intercept any wire, oral, or
5 electronic communication. Fla. Stat. § 934.03(1)(a).

6 95. Florida is an all-party-consent jurisdiction. It is lawful to intercept a wire, oral, or
7 electronic communication only “when all of the parties to the communication have given prior
8 consent to such interception.” Fla. Stat. § 934.03(2)(d). The FSCA further makes it independently
9 “unlawful to intercept any wire, oral, or electronic communication for the purpose of committing
10 any criminal act.” Fla. Stat. § 934.03(2)(e).

11 96. Meta intentionally intercepted the wire, oral, and electronic communications of the
12 Florida Subclass Members by capturing audio and video data through the Meta AI Glasses and
13 transmitting that data to its servers and to Sama's annotation facilities—without obtaining the
14 consent of all parties to those communications.

15 97. Florida Subclass Members did not consent to the interception of their
16 communications by Meta's data annotation subcontractor Sama. Florida Subclass Members did not
17 consent to having their voice recordings, video footage, and private conversations transmitted to
18 human reviewers in Kenya. The FSCA's all-party-consent requirement demands affirmative
19 consent from every person whose communication is intercepted—consent that Meta never
20 obtained.

21 98. Pursuant to Fla. Stat. § 934.10, Plaintiff and the Florida Subclass are entitled to
22 recover: (a) preliminary, equitable, or declaratory relief; (b) actual damages, but not less than
23 liquidated damages computed at the rate of \$100 per day for each day of violation or \$1,000,
24 whichever is higher; (c) punitive damages; and (d) reasonable attorneys' fees and litigation costs.

25 **THIRD CAUSE OF ACTION**
26 **Intrusion Upon Seclusion**
27 **On Behalf of Plaintiff and the Nationwide Class**

1 99. Plaintiff re-alleges and incorporates paragraphs 1 through 81 above as if fully
2 restated herein.

3 100. The Restatement (Second) of Torts § 652B provides that “[o]ne who intentionally
4 intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or
5 concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be
6 highly offensive to a reasonable person.”

7 101. Meta intentionally intruded upon Plaintiff's and Class Members' solitude and
8 seclusion by: (a) intercepting and recording their private audio and video communications through
9 the Meta AI Glasses; (b) transmitting that footage—including recordings of nudity, sexual activity,
10 bathroom visits, and private conversations—to its cloud servers; (c) routing that footage to Sama's
11 annotation facilities in Nairobi, Kenya, where human workers manually viewed the recordings in
12 full resolution; and (d) using the annotated data to train and refine Meta's AI models and enhance
13 its advertising business.

14 102. Plaintiff and Class Members had a reasonable expectation of privacy in their homes,
15 bathrooms, bedrooms, and private conversations. The types of footage described herein—nudity,
16 sexual activity, bathroom visits, bank card exposure, and intimate conversations—are among the
17 most private categories of human experience.

18 103. Meta's intrusion is highly offensive to a reasonable person. Recording a person
19 undressing or using the bathroom in their own home, transmitting that footage across the internet
20 to a server farm, and routing it to a warehouse in Kenya where strangers manually view, label, and
21 annotate the content—all to train a commercial AI product—is conduct that shocks the conscience.

22 104. Meta's intrusion is made more offensive by: (a) the vast scale of the surveillance,
23 involving millions of users across the United States; (b) the intimacy of the footage, which captures
24 people in their most vulnerable private moments; (c) Meta's active concealment of the scope and
25 nature of the human review; (d) Meta's deliberate removal of opt-out mechanisms in April 2025;
26 (e) the cross-border transfer of intimate footage to a third-party contractor in a country with no
27 EU-equivalent data protection adequacy determination; and (f) Meta's acknowledged failure to
28 reliably anonymize the footage before human review.

1 105. Meta's conduct caused Plaintiff and Class Members harm, including violation of
2 their privacy interests, emotional distress, and loss of control over highly intimate personal
3 information.

4 106. Plaintiff and Class Members seek compensatory damages, disgorgement of profits,
5 and punitive damages. Meta's conduct was willful, knowing, and carried out with conscious
6 disregard for Plaintiff's and Class Members' rights.

7 **FOURTH CAUSE OF ACTION**
8 **Unjust Enrichment**
9 **On Behalf of Plaintiff and the Nationwide Class**

10 107. Plaintiff re-alleges and incorporates paragraphs 1 through 81 above as if fully
restated herein and pleads this claim in the alternative to the legal remedies alleged herein.

11 108. Meta received substantial benefits from Plaintiff and Class Members in the form of
12 their private audio, video, and electronic communications. Meta acquired this data without
13 adequate notice or consent and without providing corresponding compensation.

14 109. Meta used this private data for its own commercial benefit, including: training and
15 refining its Llama AI models; improving its Meta AI assistant; enhancing its advertising targeting
16 capabilities through the AI-driven Advantage+ platform; and increasing the value of its products
17 and services. Meta's AI Glasses data pipeline directly fed the monetization flywheel that generated
18 over \$200 billion in annual revenue in fiscal year 2025.

19 110. Had Plaintiff and Class Members known the true scope of Meta's data practices—
20 including that their most intimate moments would be viewed by human annotators in Kenya—
21 they would not have purchased the Glasses or used the AI features, and they would not have agreed
22 to Meta's collection and use of their data.

23 111. Meta unjustly retained these benefits at the expense of Plaintiff and Class Members.
24 It is inequitable under principles of unjust enrichment for Meta to retain the profits and other
25 benefits derived from its unauthorized interception and exploitation of Plaintiff's and Class
26 Members' private communications.

27 112. Meta should be compelled to disgorge these profits and other inequitable proceeds
28 in a common fund for the benefit of Plaintiff and Class Members.

V. PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court enter an Order:

- a. Certifying the Nationwide Class and Florida Subclass and appointing Plaintiff as Class Representative;
- b. Appointing Plaintiff's counsel as Class Counsel;
- c. Finding Meta's conduct unlawful;
- d. Awarding injunctive and declaratory relief, including an order permanently enjoining Meta from intercepting, recording, transmitting, storing, or disclosing Plaintiff's and Class Members' private communications without lawful consent, requiring Meta to delete all footage obtained in violation of law, and further requiring Meta to provide clear, conspicuous notice of any human review of AI Glasses recordings and meaningful mechanisms to disable or limit such review;
- e. Awarding statutory damages under 18 U.S.C. § 2520 to Plaintiff and the Nationwide Class;
- f. Awarding statutory damages under Fla. Stat. § 934.10 to Plaintiff and the Florida Subclass;
- g. Awarding compensatory, actual, and nominal damages;
- h. Awarding punitive damages;
- i. Awarding disgorgement of all profits and revenues Meta obtained through its unlawful conduct;
- j. Awarding pre- and post-judgment interest as provided by law;
- k. Awarding reasonable attorneys' fees, costs, and expenses; and
- l. Granting such other and further relief as the Court deems just and proper.

1 Dated: March 9, 2026

/s/ Kristen Lake Cardoso

Kristen Lake Cardoso (SBN 338762)

KOPELOWITZ OSTROW P.A.

One W Las Olas Blvd, Suite 500

Fort Lauderdale, FL 33301

Tel: (954) 525-4100

cardoso@kolawyers.com