

1 Robert C. Schubert #62684  
2 Willem F. Jonckheer #178748  
3 Amber L. Schubert #278696  
4 **SCHUBERT JONCKHEER &**  
5 **KOLBE LLP**  
6 2001 Union Street, Suite 200  
7 San Francisco, CA 94123  
8 Tel: (415) 788-4220  
9 Fax: (415) 788-0161  
10 rschubert@sjk.law  
11 wjonckheer@sjk.law  
12 aschubert@sjk.law

Christian Levis (*pro hac vice* forthcoming)  
Amanda Fiorilla (*pro hac vice* forthcoming)  
Rachel Kesten (*pro hac vice* forthcoming)  
Katherine Boyd (*pro hac vice* forthcoming)  
**LOWEY DANNENBERG, P.C.**  
44 South Broadway, Suite 1100  
White Plains, NY 10601  
Tel: (914) 997-0500  
Fax: (914) 997-0035  
clevis@lowey.com  
afiorilla@lowey.com  
rkesten@lowey.com  
kboyd@lowey.com

13 *Attorneys for Plaintiffs and the Proposed Class*

14 **UNITED STATES DISTRICT COURT**  
15 **NORTHERN DISTRICT OF CALIFORNIA**

16 AIMEE STEARNS and ERIC YEPEZ,  
17 individually and on behalf of all others  
18 similarly situated,

19 Plaintiffs,

20 v.

21 META PLATFORMS, INC., SAMASOURCE  
22 IMPACT SOURCING INC., AND  
23 LUXOTTICA OF AMERICA, INC.

24 Defendants.

Case No.: 3:26-cv-02237

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

25 Plaintiffs Aimee Stearns and Eric Yopez (“Plaintiffs”), individually and on behalf of all  
26 others similarly situated, assert the following against Defendants Meta Platforms, Inc. (f/k/a  
27 Facebook, Inc.) (“Meta”), Samasource Impact Sourcing Inc. (d/b/a Sama) (“Sama”), and Luxottica  
28 of America, Inc. (“Luxottica”) (collectively, “Defendants”) based upon personal knowledge, where  
applicable, information and belief, and the investigation of counsel.

**SUMMARY OF ALLEGATIONS**

1  
2 1. This case concerns the collection, use, and disclosure of consumers’ videos, audio,  
3 and other private data by one of the largest advertising companies in the world.

4 2. This conduct starts with Meta “smart” glasses (hereinafter, “Meta Smart Glasses”),  
5 which Meta develops and sells through a partnership with Luxottica. The Meta Smart Glasses look  
6 like typical sunglasses or reading glasses, but have cameras built-in so that consumers can capture  
7 video, audio, and other content without needing to use a traditional camera or a smartphone.  
8 Consumers can enable the recording feature by saying the “wake-word” (“Hey Meta”) or by  
9 pressing a button on the glasses themselves.

10 3. At no point did Meta or Luxottica disclose that these glasses served an entirely  
11 different purpose: to capture private video, audio, and other content for profit, including to train  
12 artificial intelligence (AI) models. To the contrary, they promised the exact opposite, repeatedly  
13 touting that the Meta Smart Glasses were designed with “privacy” in mind and that consumers could  
14 at all times control what videos, audio, or data were shared through the Meta Smart Glasses and  
15 ultimately used by Meta.

16 4. Each of these promises was a lie. Meta used consumers’ audio and visual recordings  
17 captured through the Meta Smart Glasses to train its AI models, including videos and audio that  
18 were captured when consumers did not say the wake-word or otherwise enable the video and audio  
19 recording function. Consumers were never told Meta would use their private data for this purpose,  
20 and certainly not when they themselves did not trigger this functionality.

21 5. This conduct is particularly problematic because, once data enters Meta’s systems,  
22 there are no controls over how this data is used or where it goes, nor is there any way to truly delete  
23 it. Thus, consumers can never ensure their data is no longer used and have lost all control over this  
24 private information.

25 6. And, worse, Meta not only stored and used this audio and video content, but it  
26 contractually agreed with a third party—Sama—to have independent contractors stationed in Kenya  
27 manually review and annotate these videos specifically to improve its AI capabilities. These  
28

1 annotations were also stored and used by Meta, all while compounding the privacy harms to  
2 individual consumers.

3 7. Indeed, many of these contractors recently revealed to journalists just how  
4 problematic their human review of these videos and audio are and how it made even *them* feel  
5 uncomfortable. The consumers whose private videos and audio were captured, especially without  
6 triggering the Meta Smart Glasses’ recording function, never expected to have their privacy intruded  
7 in this manner.

8 8. As explained by one contractor, it feels like they are looking straight into people’s  
9 private lives, “[b]ut since it is a job, you have to do it. You understand that it is someone’s private  
10 life you are looking at, but at the same time you are just expected to carry out the work. You are not  
11 supposed to question it. If you start asking questions, you are gone.”<sup>1</sup>

12 9. These contractors also explained the private video recordings they were tasked with  
13 reviewing—through Sama and Meta’s agreement—revealed extremely personal matters, from  
14 nudity, to sexual acts, as well as credit card information. The same goes for audio. One contractor  
15 explained, “[w]e see chats where someone talks about crimes or protests . . . it can be very dark  
16 things[.]” No consumers expected other humans would ever see their private videos or chat  
17 conversations.

18 10. Many of these contractors explained their work makes them uncomfortable,  
19 particularly because they are annotating videos that consumers do not know were recorded. For  
20 instance, one contractor explained a man took *off* his Meta Smart Glasses and left them on a table,  
21 only for the glasses to record his wife after she came into the room to change her clothes, showing  
22 her naked.<sup>2</sup>

23 11. Meta and Luxottica have sold over seven million Meta Smart Glasses just last year,  
24 with plans to double production. Meta and Luxottica continue to misrepresent, and fail to disclose,

---

25 <sup>1</sup> Naipanoi Lepapa, *et al.*, *She Came Out of the Bathroom Naked, Employee Says*, SVENSKA  
26 DAGBLADET (Feb. 27, 2026), <https://www.svd.se/a/K8nrV4/met-as-ai-smart-glasses-and-data-privacy-concerns-workers-say-we-see-everything>.

27 <sup>2</sup> *Id.*

1 the true nature and purpose of these glasses: to obtain private video and audio content Meta would  
2 not otherwise have access to, including to train and profit from its AI models. Indeed, they continue  
3 to tout that the Meta Smart Glasses are “[d]esigned for privacy” and “controlled” by the consumer.

4 12. Defendants’ interception, use, and disclosure of this information without  
5 consumers’ consent—at a minimum—constitutes an extreme invasion of Plaintiffs’ and Class  
6 Members’ privacy. It also violates each of the laws described herein.

7 13. Given the secret and undisclosed nature of Defendants’ conduct, additional  
8 evidence supporting Plaintiffs’ claims, including the full extent of the sensitive personal information  
9 Defendants intercepted, and how they used that information, will be revealed in discovery.

10 **PARTIES**

11 **A. Plaintiffs**

12 14. **Plaintiff Aimee Stearns** is a resident of Fresno County, California.

13 15. Plaintiff Stearns purchased first-generation Ray-Ban Stories in approximately 2021,  
14 second-generation Ray-Ban Meta Smart Glasses in approximately 2024, and Oakley Vanguard Meta  
15 Smart Glasses in January 2026.

16 16. Plaintiff Stearns uses her Meta Smart Glasses at least once a month.

17 17. Unbeknownst to Plaintiff Stearns, Defendants collectively intercepted, used, and  
18 disclosed the content of her private video and audio recordings.

19 18. Plaintiff Stearns did not consent to the sharing, use, and interception of her private  
20 data, or the use of this information by Defendants or anyone else.

21 19. Defendants’ interception, use, and disclosure of the content of Plaintiff Stearns’  
22 private video, audio, and other data were undoubtedly privacy invasive, deprived her of the value  
23 of her own data, and caused her to pay more for her Meta Smart Glasses than she otherwise would  
24 have.

25 20. **Plaintiff Eric Yopez** is a resident of Fresno County, California.

26 21. Plaintiff Yopez purchased Meta Smart Glasses on January 6, 2026.

27 22. Plaintiff Yopez uses his Meta Smart Glasses nearly every day.

1 23. Unbeknownst to Plaintiff Yepez, Defendants collectively intercepted, used, and  
2 disclosed the content of his private video and audio recordings.

3 24. Plaintiff Yepez did not consent to the sharing, use, and interception of his private  
4 data, or the use of this information by Defendants or anyone else.

5 25. Defendants' interception, use, and disclosure of the content of Plaintiff Yepez's  
6 private video, audio, and other data were undoubtedly privacy invasive, deprived him of the value  
7 of his own data, and caused him to pay more for his Meta Smart Glasses than he otherwise would  
8 have.

9 **B. Defendants**

10 26. **Defendant Meta Platforms, Inc.** is a Delaware corporation with its principal place  
11 of business located in Menlo Park, California.

12 27. Meta, as the creator and developer of Meta AI and the Meta Smart Glasses, was at  
13 all times aware of the privacy implications in recording and capturing consumers' private videos.

14 28. Indeed, Meta went to great lengths to reassure consumers and regulators that its  
15 conduct was privacy-compliant, including repeatedly touting its privacy settings and stringent  
16 vetting process for releasing new products and features.

17 29. This includes express representations that the Meta Smart Glasses were designed  
18 with “[p]rivacy . . . built-in.”<sup>3</sup> Meta promised that it adhered to “best practices and [met] high  
19 standards for data protection.”<sup>4</sup> And, importantly, Meta promised that it would ensure “that people  
20 understand the types of data we use to train the models that power our generative AI products.”<sup>5</sup>

21 30. Meta, at all times, knew that it captured, intercepted, used, and stored consumers'  
22 private audio, video, and other private data because it controlled every part of this process, including  
23 contracting with Sama to review and annotate these videos.

24 \_\_\_\_\_  
25 <sup>3</sup> META, *Introducing Ray-Ban Stories: First-Generation Smart Glasses* (Sept. 9, 2021),  
<https://about.fb.com/news/2021/09/introducing-ray-ban-stories-smart-glasses/>.

26 <sup>4</sup> META, *Building Generative AI Features Responsibly* (Sept. 27, 2023),  
<https://about.fb.com/news/2023/09/building-generative-ai-features-responsibly/>.

27 <sup>5</sup> *Id.*

1 31. As such, Meta’s conduct was intentional despite knowing the privacy violations it  
2 caused to Plaintiffs and Class Members.

3 32. **Defendant Luxottica of America, Inc.** is an Ohio corporation with its principal  
4 place of business in Mason, Ohio.

5 33. Luxottica partnered with Meta to offer each and every version of the Meta Smart  
6 Glasses. Meta could not have sold its privacy-invasive smart glasses if not for Luxottica.

7 34. Indeed, *The Verge* reported back in 2021 that it was Luxottica’s Chief Wearable  
8 Officer, Rocco Basilico, who *cold emailed* Meta’s Chief Executive Officer (“CEO”), Mark  
9 Zuckerberg, to first discuss a collaboration for smart glasses.<sup>6</sup> Mr. Zuckerberg then flew to Milan to  
10 meet with Luxottica’s founder and chairman, Leonardo Del Vecchio, to discuss and agree to this  
11 joint venture.<sup>7</sup> The same report explains that many of the Meta Smart Glasses “features”—  
12 codenamed “Stella” at the time—were collaboratively developed with high-level executives from  
13 both corporate entities. The launch of Meta Smart Glasses can be described as nothing other than a  
14 fully collaborative, joint venture.

15 35. As a well-established corporate entity, Luxottica would not have developed and  
16 offered this product to consumers without knowing precisely how it functioned or the privacy  
17 concerns associated with this product, including the unlawful use, collection, and disclosure of  
18 consumers’ data and private video and audio recordings.

19 36. Notably, both Ireland’s Data Protection Commission and Italy’s privacy watchdog,  
20 the Garante, raised concerns about these glasses the same year they were first offered for sale.<sup>8</sup>

21  
22 <sup>6</sup> Alex Heath, *Facebook on Your Face*, THE VERGE (Sept. 9, 2021),  
23 <https://www.theverge.com/2021/9/9/22662809/facebook-ray-ban-stories-camera-smart-glasses-hands-on>.

24 <sup>7</sup> *Id.*

25 <sup>8</sup> Irish Data Protection Comm’n, *Data Protection Commission Concerning Facebook View (glasses)*  
26 (Sept. 17, 2021), <https://www.dataprotection.ie/en/news-media/latest-news/data-protection-commission-statement-concerning-facebook-view-glasses>; REUTERS, *Ireland Raises Privacy Question Over Facebook Smart Glasses* (Sept. 17, 2021),  
27 <https://www.reuters.com/technology/ireland-raises-privacy-question-over-facebook-smart-glasses-2021-09-17/>.

1 37. Amnesty International’s technology division, called Amnesty Tech, raised similar  
2 concerns. It posted on Twitter (now X) back in 2021: “Facebook is a surveillance advertising  
3 company whose business relies on exploiting our data and invading our privacy on a vast scale.” It  
4 continued: “Now it has teamed up with Ray-Ban to sell camera glasses. *@ray\_ban have you thought*  
5 *this through?*”<sup>9</sup> Ray Ban is one of the glasses brands offered by Luxottica, and the first brand to  
6 offer Meta Smart Glasses.

7 38. Luxottica must have known, and ignored, these privacy concerns in continuing to  
8 partner with Meta and offer the Meta Smart Glasses for years on end.

9 39. As such, Luxottica’s conduct was intentional despite knowing the privacy violations  
10 it caused to Plaintiffs and Class Members.

11 40. **Defendant Samasource Impact Sourcing Inc.** is a Delaware corporation with its  
12 principal place of business in San Francisco, California.

13 41. Sama provides facilities and contractors to perform data annotation, including  
14 manually reviewing video and voice recordings, and labeling this video and audio content. Sama  
15 performs this work specifically to enhance the data’s utility for AI modeling.

16 42. Sama secured \$70 million in Series B funding, following \$14.8 million in Series A  
17 funding. Its corporate mission is to develop an end-to-end platform to get data, annotate it, and  
18 enable it to be used for AI modeling.<sup>10</sup>

19 43. Sama has worked with Meta, Google, Walmart, and Nvidia, among other large  
20 corporate clients.<sup>11</sup> As part of its work, Sama works directly with these customers to understand  
21 their business needs and sources of data. As explained by its CEO and founder, Leila Janah, “In  
22 some cases we might refine elements of our software . . . then we go into deployment and . . .  
23

24 <sup>9</sup> AmnestyTech (@AmnestyTech), X, (Sept. 9, 2021, 9:56 AM PST),  
25 <https://x.com/AmnestyTech/status/1436010618318958594?s=20> (emphasis added).

26 <sup>10</sup> Christine Hall, *Sama Taps Into \$70M to Build ‘First End-to-End AI Platform’ for Training Data*,  
27 TECHCRUNCH (Nov. 4, 2021), <https://techcrunch.com/2021/11/04/sama-taps-into-70m-to-build-first-end-to-end-ai-platform-for-training-data/>.

28 <sup>11</sup> *Id.*

1 annotation work[.]”<sup>12</sup> Thus, at all times, Sama is aware of where data comes from and the purposes  
2 for which companies contract for its services.

3 44. Sama contracted with Meta to review private video and audio recordings captured  
4 on Meta Smart Glasses, which it performed from its facility in Nairobi, Kenya.

5 45. Sama knew that the video, audio, and other data its contractors were reviewing were  
6 objectively private, including inherently intimate conduct like sexual acts.

7 46. Sama went to great lengths to avoid its contractors from disclosing this conduct,  
8 including requiring contractors to sign extensive non-disclosure agreements.

9 47. As such, Sama’s conduct was intentional despite knowing the privacy violations it  
10 caused to Plaintiffs and Class Members.

11 **JURISDICTION AND VENUE**

12 48. This Court has jurisdiction over the subject matter of this action pursuant to 28  
13 U.S.C § 1332(d), because the amount in controversy for the Classes exceeds \$5,000,000 exclusive  
14 of interest and costs, there are more than 100 putative members of the Classes defined below, and a  
15 significant portion of putative Class Members are citizens of a state different from the Defendants.

16 49. This Court has personal jurisdiction over Meta and Sama because their principal  
17 places of business are in California. Luxottica is also subject to specific personal jurisdiction in this  
18 State because a substantial part of the events and conduct giving rise to Plaintiffs’ claims occurred  
19 in this State, including the interception, use, and disclosure of Plaintiffs’ private communications  
20 and interactions and use of that data for commercial purposes.

21 50. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(b), (c), and (d)  
22 because a substantial portion of the conduct described in this Class Action Complaint was carried  
23 out in this District.

24 51. **Divisional Assignment:** This action arises in San Mateo County, in that a  
25

---

26 <sup>12</sup> Jake Bright, *Samasource raises \$14.8M for global AI data biz driven from Africa*, TECHCRUNCH  
27 (Nov. 20, 2019), <https://techcrunch.com/2019/11/20/samasource-raises-14-8m-for-global-ai-data-biz-driven-from-africa/>.

1 substantial part of the events which give rise to the claims asserted herein occurred in San Mateo  
2 County. Pursuant to L.R. 3-2(d), all civil actions that arise in San Mateo County shall be assigned  
3 to the San Francisco or Oakland Division.

4 **FACTUAL BACKGROUND**

5 **A. Background of Meta’s Advertising Business**

6 52. Meta is one of the largest advertising companies in the country. To date, Meta  
7 generates nearly 98% of its revenue through advertising bringing in a grand total of \$200.97 billion.

8 53. Meta’s advertising business began back in 2007 with the creation of “Facebook  
9 Ads,” which was marketed as a “completely new way of advertising online” that would allow  
10 “advertisers to deliver more tailored and relevant ads.”

11 54. Meta’s advertising business has been extremely successful due, in large part, to  
12 Meta’s ability to target people at a granular level. “Among many possible target audiences, [Meta]  
13 offers advertisers,” for example, “1.5 million people ‘whose activity on Facebook suggests that  
14 they’re more likely to engage with/distribute liberal political content’ and nearly seven million  
15 Facebook users who ‘prefer high-value goods in Mexico.’”<sup>13</sup>

16 55. Today, Meta provides advertising on its own platforms, such as Facebook and  
17 Instagram, as well as other websites through the Facebook Audience Network.

18 56. Facebook alone has more than three billion active users. All of Meta’s products,  
19 including Facebook and Instagram, are designed to keep individuals in the Meta ecosystem where  
20 Meta can serve more ads, target more consumers, and make more money.

21 57. Meta’s AI capabilities are no exception. Meta began making significant investments  
22 in AI as early as 2013, many of which were developed to boost its advertising business and its ability

23  
24  
25  
26 <sup>13</sup> Natasha Singer, *What You Don’t Know About How Facebook Uses Your Data*, N.Y. TIMES (Apr.  
27 11, 2018), <https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html>.

1 to target individual consumers.<sup>14</sup> Indeed, in 2025, Meta’s CEO, Mark Zuckerberg, announced that  
2 it was planning to launch an end-to-end AI advertising tool.<sup>15</sup> Per Mr. Zuckerberg: “The basic end  
3 goal here is any business can come to us, say what their objective is — we get new customers to do  
4 this thing, or sell these things — tell us how much they’re willing to pay to achieve those results,  
5 connect their bank account, and then we just deliver as many results as we can,” he explained. “In  
6 a way, it’s kind of like the ultimate business results machine. I think it’d be one of the most important  
7 and valuable AI systems that gets built.”<sup>16</sup>

8 58. This new tool would build on Meta’s existing AI and machine learning (“ML”) capabilities,  
9 which are already capable of targeting consumers without an advertiser recommending  
10 specific demographics.<sup>17</sup> For Meta’s AI systems to have this functionality, they would need to be  
11 trained on a significant amount of ads, consumer data, and large-scale behavioral datasets capturing  
12 users’ activities, preferences, location signals, and engagement with digital content across the  
13 internet.

14 59. Meta gets this data from its own platform, as well as consumers’ off-Facebook  
15 activity through Meta’s tools and products like pixels and software development kits (“SDKs”). But  
16 that is not the only way. As described below, Meta has been using consumers’ private audio, video,  
17 and other data captured through Meta Smart Glasses to train its AI models, including submitting  
18 this private content to third-party contractors for annotation and labeling.

19 60. All this data that Meta obtains is used to identify and target individual consumers, as  
20 well as improve the tools used to target consumers and optimize ad delivery, or otherwise keep  
21 consumers on its platforms to advance these goals. As aptly put by Maxwell Zeff at *TechCrunch* in  
22

---

23 <sup>14</sup> Jill Avery & Robert J. Dolan, *Meta: Digital Marketing and Artificial Intelligence (AI) at Facebook*  
24 *and Instagram*, Harv. Bus. Sch. Teaching Note No. 526-053 (Feb. 2026),  
<https://www.hbs.edu/faculty/Pages/item.aspx?num=68063>.

25 <sup>15</sup> Maxwell Zeff, *Mark Zuckerberg’s AI Ad Tool Sounds Like a Social Media Nightmare*,  
26 *TECHCRUNCH* (May 7, 2025), <https://techcrunch.com/2025/05/07/mark-zuckerbergs-ai-ad-tool-sounds-like-a-social-media-nightmare/>.

27 <sup>16</sup> *Id.*

27 <sup>17</sup> *Id.*

1 describing Meta’s new AI ambitions, “If it wasn’t clear before that users are the product on Meta’s  
2 platforms and advertisers the customers, it’s about to become crystal.”<sup>18</sup> The Meta Smart Glasses  
3 are no exception; it is consumers who are the actual product.

4 **B. Meta’s Smart Glasses & Meta AI**

5 61. Meta’s roll out of new products are designed to do the same thing: learn more  
6 information about consumers and improve its ad-targeting capabilities. This includes Meta’s AI-  
7 powered smart glasses, i.e., Meta Smart Glasses.

8 62. In September 2021, Meta announced Ray-Ban Stories, the first-generation model of  
9 the Meta Smart Glasses that were built through a partnership with Luxottica.<sup>19</sup> These glasses were  
10 sold for \$299. Each pair came with a built-in camera system that allowed consumers to “capture  
11 photos and video” directly through their glasses, rather than relying on a standalone camera or their  
12 smartphone.

13 63. The Meta Smart Glasses include a small white LED on the frame that illuminates  
14 when the camera records or takes a photo. However, regulators, researchers, and media reports have  
15 raised concerns that this indicator may not reliably alert consumers to recordings, particularly  
16 because the light can be obscured, disabled through modifications, or otherwise overlooked.

17 64. Nevertheless, Meta and Luxottica marketed these glasses as coming with “[p]rivacy  
18 . . . built-in.”<sup>20</sup> Meta’s press release noted “[f]rom the start, we designed Ray-Ban Stories with  
19 privacy in mind, adding numerous built-in features to provide control and peace of mind to both  
20 device owners and bystanders.”

21 65. On September 27, 2023, Meta and Luxottica launched the second-generation of Meta  
22 Smart Glasses—dubbed the “Ray-Ban Meta smart glasses”—at Meta Connect. These glasses were  
23 sold for \$299 and touted as being “redesigned . . . from the ground up.”<sup>21</sup> These glasses, like its  
24

---

25 <sup>18</sup> *Id.*

26 <sup>19</sup> META, *Introducing Ray-Ban Stories: First-Generation Smart Glasses*, *supra* n.3.

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

28 <sup>21</sup> META, *Introducing the New Ray-Ban | Meta Smart Glasses* (Sept. 27, 2023)  
<https://about.fb.com/news/2023/09/new-ray-ban-meta-smart-glasses/>.

1 predecessor, still allowed consumers to capture videos and pictures manually, including by pressing  
2 a button on the glasses themselves. However, one major improvement to the Meta Smart Glasses  
3 was the incorporation of “Meta AI” announced the same day.<sup>22</sup>

4 66. Meta AI is Meta’s “advanced conversational assistant.” It was launched with the  
5 Meta Smart Glasses, as well as across other Meta platforms, including WhatsApp, Messenger, and  
6 Instagram.<sup>23</sup>

7 67. Meta AI is powered by Meta’s “llama” models and LLM research. When a consumer  
8 prompts Meta AI to answer a question, Meta AI accesses real-time information through a partnership  
9 it has with Bing.<sup>24</sup> As of 2024, it was reported that Meta was developing its own search tool for  
10 Meta AI to decrease its reliance on Bing for this service.

11 68. Consumers who purchased second-generation Meta Smart Glasses can interact with  
12 Meta AI by saying “Hey Meta.” This “Hey Meta” functionality is particularly error-prone and can  
13 capture audio and video without consumers’ knowledge.

14 69. Meta Smart Glasses consumers are prompted on how to use Meta AI during the  
15 device set-up process.

16  
17  
18  
19 \* \* \*

20  
21  
22  
23  
24  
25 

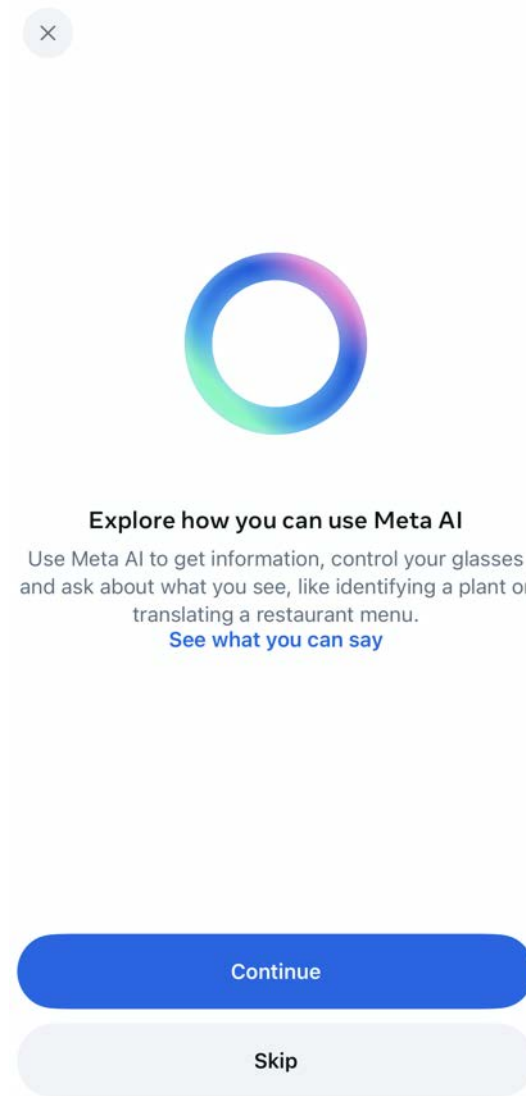
---

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

26 <sup>23</sup> META, *Introducing New AI Experiences Across Our Family of Apps and Devices* (Sept. 27, 2023)  
27 [https://about.fb.com/news/2023/09/introducing-ai-powered-assistants-characters-and-creative-  
tools/](https://about.fb.com/news/2023/09/introducing-ai-powered-assistants-characters-and-creative-tools/).

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

**FIGURE 1**



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

70. Like with its first-generation smart glasses, Meta promised that—with respect to Meta AI and Meta AI-powered products—it was “committed to building responsibility with safety in mind.”<sup>25</sup> Meta claimed they were “held accountable for protecting people’s privacy by regulators, policymakers, and experts” and that it “work[ed] with them to ensure that [Meta] . . . follows best practices and meets high standards for data protection.” This includes ensuring “that people

---

<sup>25</sup> *Id.*

1 understand the types of data we use to train the models that power our generative AI products.”<sup>26</sup> It  
2 also assured users that it built “important privacy safeguards” and that each of its “generative AI  
3 features go through a rigorous internal privacy review” to “ensure [Meta is] using people’s data  
4 responsibly.”<sup>27</sup>

5 71. In April 2024, Meta announced a new update for its Meta Smart Glasses that were  
6 again built in partnership with Luxottica. Among the new features, consumers could now share their  
7 view on video calls via WhatsApp and Messenger hands-free. And, more significantly, Meta touted  
8 that it made its smart glasses “[e]ven [s]marter.”<sup>28</sup> Now, not only could consumers use Meta AI to  
9 get real-time answers to questions, but Meta AI could—through the camera feature—see what  
10 consumers were seeing. For example, if a consumer was viewing text in a foreign language, they  
11 could ask Meta AI to translate the text to their native language. Likewise, if a consumer was viewing  
12 an object, they could ask Meta AI to identify it or describe what they are seeing.<sup>29</sup> Meta AI can also  
13 place calls, send messages, and scan QR codes.

14 72. In June 2025, Meta released additional Meta Smart Glasses, this time with Oakley,  
15 another Luxottica brand. These glasses function the same as Meta’s Ray-Ban-branded smart glasses  
16 but allow for longer recordings and longer battery life.<sup>30</sup> The Oakley Meta Smart Glasses include  
17 the Oakley Meta Vanguard and Oakley Meta HTSN.

18 73. In September 2025, Meta launched the Meta Ray-Ban Display. This new version of  
19 the Meta Smart Glasses line allows consumers to interact with a screen built into the glasses  
20  
21

---

22 <sup>26</sup> META, *Building Generative AI Features Responsibly*, *supra* n.4.

23 <sup>27</sup> Mike Clark, *Privacy Matters: Meta’s Generative AI Features*, META (Sept. 27, 2023)  
24 <https://about.fb.com/news/2023/09/privacy-matters-metas-generative-ai-features/>.

25 <sup>28</sup> META, *New Ray-Ban | Meta Smart Glasses Styles and Meta AI Updates* (Apr. 23, 2024),  
26 <https://about.fb.com/news/2024/04/new-ray-ban-meta-smart-glasses-styles-and-meta-ai-updates/>.

27 <sup>29</sup> *Id.*

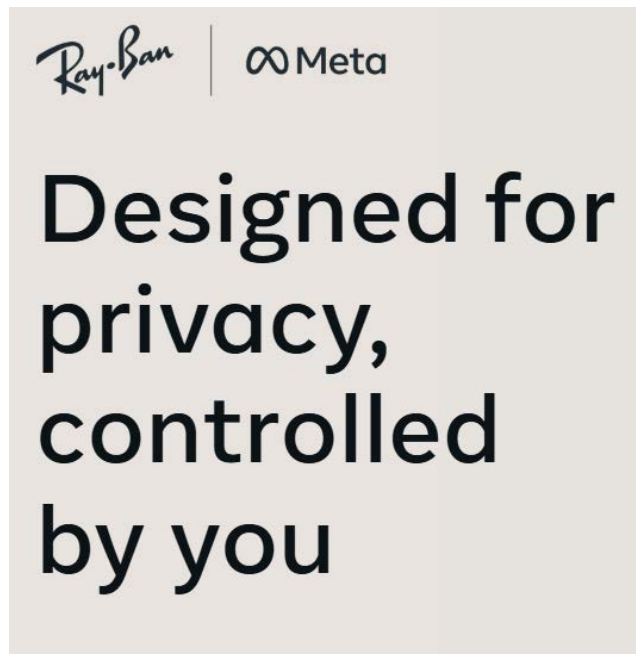
28 <sup>30</sup> META, *Introducing Oakley Meta Glasses, a New Category of Performance AI Glasses* (June 20,  
2025), <https://about.fb.com/news/2025/06/introducing-oakley-meta-glasses-a-new-category-of-performance-ai-glasses/>.

1 themselves. Consumers can navigate a menu displayed on the screen through a wristband, using  
2 their fingers to tap on menu options and swipe through various features.<sup>31</sup>

3 74. Meta and Luxottica have sold over seven million smart glasses in 2025 alone, with a  
4 particularly strong demand in the U.S. market.<sup>32</sup> In 2023 and 2024, the companies sold two million  
5 units. Both companies are considering doubling production going forward.

6 75. All the while, Meta has continued to tout its privacy protections. For instance, the  
7 Meta's Ray-Ban branded smart glasses website prominently displays "Designed for privacy,  
8 controlled by you."<sup>33</sup> See **Figure 2**.

9 **FIGURE 2**



23  
24  
25  
26

<sup>31</sup> ONOFF.GR, *Meta Smart Glasses: Record-Breaking 7 Million Sales* (Feb. 19, 2026), [https://www.onoff.gr/blog/en/metaverse-vr/meta-smart-glasses-poliseis-rekor/#:~:text=Meta%20Smart%20Glasses:%20Record%2DBreaking%207%20Million%20Sales,Evolution.%20\\*%2026%20Starting%20Price%20\(Gen%202\)](https://www.onoff.gr/blog/en/metaverse-vr/meta-smart-glasses-poliseis-rekor/#:~:text=Meta%20Smart%20Glasses:%20Record%2DBreaking%207%20Million%20Sales,Evolution.%20*%2026%20Starting%20Price%20(Gen%202).).

<sup>32</sup> *Id.*

<sup>33</sup> META, *Designed for Privacy, Controlled by You*, <https://www.meta.com/ai-glasses/privacy/> (last visited Mar. 13, 2026).

1 76. It also represents that consumers are “in control of your data and content” and can  
2 “choose” what to “share with others, and when.”<sup>34</sup> See **Figure 3**. Meta promises that it provides  
3 “[e]asy to access settings” that let consumers “manage the information you share with Meta.”<sup>35</sup>

4 **FIGURE 3**

5  
6 **You’re in  
7 control  
8 of your  
9 data and  
10 content.**

11  
12  
13 Clear, easy device and  
14 app settings help you  
15 manage your  
16 information, giving you  
17 control over what  
18 content you choose to  
19 share with others, and  
20 when.



21 **Privacy Settings that matter**

22  
23 Easy to access settings let you view and  
24 manage the information you share with Meta.  
25 Meta collects data needed to help ensure  
26 your glasses and app are reliable, secure, and  
27 operating normally. You can choose to share  
28 additional data to improve the experience.

29 77. Acknowledging the privacy implications with taking videos without consumers’  
30 consent, Meta tells its customers to wear “Ray-Ban Meta glasses responsibly.”<sup>36</sup> This includes

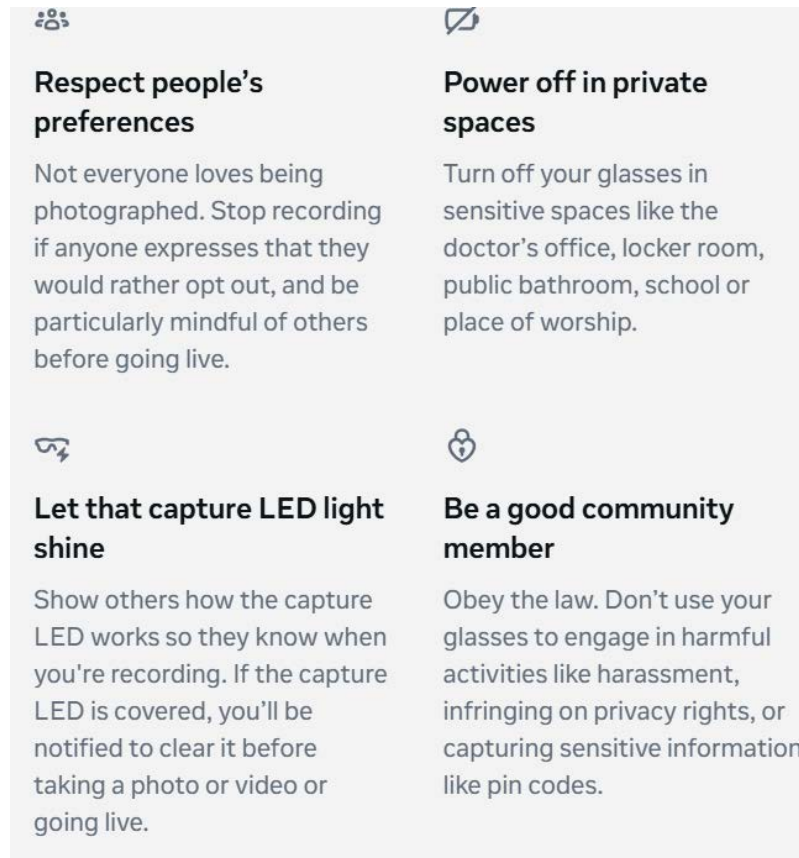
31  
32  
33  
34 *Id.*

35 *Id.*

36 *Id.*

1 “[r]espect[ing] people’s preferences” because “[n]ot everyone loves being photographed” such that  
 2 consumers should “[s]top recording if anyone expresses that they would rather opt out.”<sup>37</sup> It also  
 3 recommends consumers “[t]urn off [their] glasses in sensitive spaces” to further respect the privacy  
 4 rights of other individuals, including “doctor’s office[s]” and “locker room[s].”<sup>38</sup> Likewise, it tells  
 5 consumers to “[o]bey the law” and not to “use” the “glasses to engage in harmful activities like . . .  
 6 infringing on privacy rights” or to “captur[e] sensitive information like pin codes.”<sup>39</sup>

7 **FIGURE 4**



22  
 23 78. Consumers have no reason to suspect that Meta would collect, share, or use their  
 24 private videos and audio to train AI or take videos without their consent. This is especially true in

25  
 26 <sup>37</sup> *Id.*

27 <sup>38</sup> *Id.*

28 <sup>39</sup> *Id.*

1 light of Meta’s repeat promises that consumers were ultimately in control of their glasses and all  
2 videos, audio, and data associated with them. But despite these promises—and repeat insistence that  
3 *consumers* obey the law—Defendants did not do so.

#### 4 C. Meta’s Violations of Consumers’ Privacy

5 79. Meta’s Privacy Center represents that Meta AI is powered by (1) “public content”  
6 like “profile info, comments, and posts”; (2) “interactions with AI features” like “questions you ask  
7 and images you ask Meta AI to imagine for you”; (3) other “public sources on the internet”; (4)  
8 “[i]nformation from partners”; and (5) “[l]icensed information.”<sup>40</sup>

9 80. Nowhere in this policy does Meta disclose that it will capture, use, and disclose  
10 consumers’ private interactions, captured through Meta Smart Glasses, for AI training.

11 81. Meta also claims it takes steps to “limit the possibility of private information that  
12 you may share with generative AI features” from being shared with “other people.”<sup>41</sup> And it  
13 promises consumers can also permanently delete their information so “it won’t be used for future  
14 training.”<sup>42</sup>

15 82. None of this was true. Nor are Meta’s other privacy promises.

16 83. In a February 27, 2026 report, a Swedish newspaper revealed that Meta has a  
17 subcontractor, Sama, with facilities in Nairobi, Kenya whose contractors are tasked with manually  
18 labeling images, videos, and audio captured through Meta Smart Glasses to train AI. These  
19 employees are known as data annotators.<sup>43</sup>

20 84. While these contractors are threatened with losing their jobs for disclosing Meta’s  
21 privacy invasions—through extensive confidentiality agreements—over thirty contractors revealed  
22 the truth of their work anonymously.

---

24 <sup>40</sup> META, *Generative AI: AI at Meta*, [https://www.facebook.com/privacy/guide/genai?entry\\_point=](https://www.facebook.com/privacy/guide/genai?entry_point=)  
25 (last visited Mar. 13, 2026).

26 <sup>41</sup> Mike Clark, *Privacy Matters: Meta’s Generative AI Features*, *supra* n.27.

27 <sup>42</sup> META, *How Generative AI Models Work*, [https://www.facebook.com/privacy/dialog/how-](https://www.facebook.com/privacy/dialog/how-generative-ai-models-work)  
28 generative-ai-models-work (last visited Mar. 13, 2026).

<sup>43</sup> Naipano Lepapa, *et al.*, *She Came Out of the Bathroom Naked, Employee Says*, *supra* n.1.

1 85. Many of these contractors explained their work makes them uncomfortable,  
2 particularly because they are annotating videos that consumers do not know were recorded. For  
3 instance, one contractor explained a man took off his Meta Smart Glasses and left them on a table,  
4 only for the Meta Smart Glasses to record his wife after she came into the room to change her  
5 clothes.

6 86. Other contractors explained the glasses capture videos of consumers in the bathroom,  
7 when they are naked, having sex, watching porn, and even financial information like bank cards.

8 87. As put by one contractor: “When you see these videos, it feels [like “you are looking  
9 straight into other people’s private lives”] [b]ut since it is a job, you have to do it. You understand  
10 that it is someone’s private life you are looking at, but at the same time you are just expected to  
11 carry out the work. You are not supposed to question it. If you start asking questions, you are  
12 gone.”<sup>44</sup>

13 88. These data annotators were tasked with not only annotating and labeling videos, but  
14 reviewing transcripts of consumers’ questions to Meta AI, which also involve sensitive materials.  
15 This data, alongside the annotations, are stored on Meta’s servers for AI training and modeling.

16 89. Additionally, several former Meta employees in the United States confirmed that  
17 “live data” is annotated and used in several projects.

18 90. Meta, and its subcontractor Sama, went to great lengths to prevent this information  
19 from getting out. As explained by one employee, “There are cameras everywhere in our office, and  
20 you are not allowed to bring your own phones or any device that can record.”<sup>45</sup>

21 91. The same researchers who broke this news also tested Meta AI-enabled glasses  
22 themselves. They found that, not only is there no ability to use the device without an internet  
23 connection enabled, but also there were consistent and frequent transmissions to Meta’s servers.<sup>46</sup>  
24  
25

---

26 <sup>44</sup> *Id.*

27 <sup>45</sup> *Id.*

28 <sup>46</sup> *Id.*

1           92. They also found that sales staff selling the Meta Smart Glasses, developed and  
2 offered through its partnership with Luxottica, were woefully unprepared to explain its data sharing  
3 activities. Indeed, they found some sales staff represented “Nothing is shared with them (Meta).  
4 That was a big concern for me as well. Are they going to get access to my data, that is a bit scary,  
5 but you have full control.”<sup>47</sup> Another admitted “[t]o be completely honest, I don’t know where the  
6 data goes, or if they take data at all.” And a final claimed “it is completely fine – everything stays  
7 locally in the app.”<sup>48</sup>

8           93. Also notably, according to reports, Meta *ignored* the journalists who had uncovered  
9 its conduct for nearly two months, before replying that “[w]hen live AI is being used, we process  
10 that media according to the Meta AI Terms of Service and Privacy Policy.”<sup>49</sup>

11           94. But none of its practices fall within Meta’s privacy promises, including its AI Terms  
12 of Service. Nothing in this document mentions using consumers’ private videos or audio recordings  
13 to train AI. Indeed, most of the policy refers to “Content” which is defined as users’ “Prompts” to  
14 AI and the AI “Output[.]” alongside any “Feedback.” For instance, asking (i.e., prompting) AI to  
15 answer a question and receiving an answer (i.e., an output). The private video and audio recordings  
16 Defendants captured, used, and disclosed to contractors do not remotely fall within Meta’s definition  
17 of “Content.”

18           95. Meta’s Privacy Policy is equally deficient. As described above, its Privacy Center  
19 lists explicit types of information used for training AI and private video and audio recordings are  
20 not one of them.

21           96. And even if one navigated through the host of disparate pages Meta provides about  
22 its data handling practices—of which there are many—they still would not learn of Meta’s

---

23 \_\_\_\_\_  
24 <sup>47</sup> *Id.*

25 <sup>48</sup> *Id.*

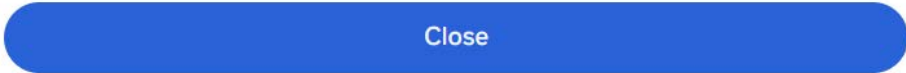
26 <sup>49</sup> Matt Growcoat, *Disturbing Report Says Workers are Watching Private Footage Taken on Meta*  
27 *Smart Glasses*, PETAPIXEL (Mar. 5, 2026), <https://petapixel.com/2026/03/05/disturbing-report-says-workers-are-watching-private-footage-taken-on-meta-smart-glasses/#:~:text=Disturbing%20Report%20Says%20Workers%20are,is%20wearing%20them%20having%20sex.%E2%80%9D>.

1 collection, sharing, and use of private videos. For instance, where Meta mentions its “camera  
 2 feature,” clicking the link to learn more only describes how Meta collects *voice* information and  
 3 *only* when Meta AI is explicitly prompted by the user to enable the Meta AI capabilities.<sup>50</sup> This does  
 4 not disclose Meta’s collection, disclosure, and use of private videos and audio when unprompted or  
 5 when consumers are not engaging with Meta AI.

6 **FIGURE 5**

7 **What we collect from voice-enabled features**

8 Ren tells Meta’s voice-enabled Assistant to take a photo on smart glasses. A  
 9 visual indicator shows that Assistant is activated and listening for Ren’s  
 10 command. We collect this voice interaction, which includes any background  
 11 sound that occurs when Ren says the command. Collecting Ren’s voice  
 12 interactions lets us provide and, depending on Ren’s settings, improve the  
 13 Assistant feature.



97. Likewise, where Meta describes information shared with Meta AI, it again refers to  
 “prompts” that are sent “to AI at Meta” as well as responses (i.e., questions and answers). Private  
 videos and audio captured through glasses in no way fall within this limited disclosure.<sup>51</sup>

<sup>50</sup> META, *Privacy Policy* (Dec. 16, 2025),  
<https://www.facebook.com/privacy/policy?subpage=1.subpage.1-YourActivityAndInformation>.

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

1 98. If there were any doubt at all, in September 2024, Meta refused to answer questions  
2 on how content captured by Meta Smart Glasses was used by Meta to train AI—a direct  
3 contradiction to their privacy-first messaging or claim that its conduct is adequately disclosed.

4 99. Anuj Kumar, a Meta senior director working directly on its AI wearables, refused to  
5 answer questions on how Meta would train AI models from content captured by consumers using  
6 Meta Smart Glasses. Point blank, Mr. Kumar stated Meta is “not publicly discussing that[.]”<sup>52</sup>

7 100. A Meta spokesperson, Mimi Huggins, confirmed the same, stating “[t]hat’s not  
8 something we typically share externally” and that Meta is “not saying either way” if any of this  
9 content was used to train AI.<sup>53</sup>

10 101. A Meta spokesperson later clarified to *TechCrunch* in October 2024 that “photos and  
11 videos captured on Ray-Ban Meta are *not* used by Meta for training as long as the user doesn’t  
12 submit them to AI.”<sup>54</sup> Thus, Meta promised that no photos or videos are used for any purposes unless  
13 Meta AI is expressly asked to analyze a video, picture, or answer a prompt.

14 102. Accordingly, Meta’s representation that its collection, use, and disclosure of private  
15 video and audio recordings fall within its existing policies are plainly false. It promised the opposite.

#### 16 **D. The Transmission & Storage of Data Captured by Meta Smart Glasses**

17 103. Consumers are prompted to download the Meta AI (previously the Meta View)  
18 mobile application to set up their Meta Smart Glasses. The glasses are paired with the consumers’  
19 mobile device using Bluetooth connectivity.

20 104. When consumers capture photos and videos with Meta Smart Glasses, Meta  
21 represents that the media is stored locally on the glasses. Consumers can then import that content to  
22 their mobile device through the Meta AI mobile application. Media transfer occurs through a

---

23 <sup>52</sup> Maxwell Zeff, *Meta Won’t Say Whether It Trains AI on Smart Glasses Photos*, TECHCRUNCH  
24 (Sept. 30, 2024), <https://techcrunch.com/2024/09/30/meta-wont-say-whether-it-trains-ai-on-ray-ban-meta-smart-glasses-photos/>.

25 <sup>53</sup> *Id.*

26 <sup>54</sup> Maxwell Zeff, *Meta Confirms It May Train Its AI on Any Image You Ask Ray-Ban Meta AI to*  
27 *Analyze*, TECHCRUNCH (Oct. 2, 2024), <https://techcrunch.com/2024/10/02/meta-confirms-it-may-train-its-ai-on-any-image-you-ask-ray-ban-meta-ai-to-analyze/> (emphasis in original).

1 wireless connection between Meta Smart Glasses and the mobile device, typically using Bluetooth  
2 and, in some cases, Wi-Fi for larger file transfers. After the media is imported to the consumer's  
3 device, it is purportedly removed from the Meta Smart Glasses' local storage. Meta Smart Glasses  
4 can also perform automatic imports if the consumer enables that feature in the Meta AI application.

5 105. When Meta AI is invoked, however, the process differs. Queries or commands  
6 directed to Meta AI—including audio, video, or other data captured by Meta Smart Glasses in  
7 connection with the request—are transmitted in real time to Meta's servers for processing to quickly  
8 generate a response. This transmission occurs contemporaneously with the capture of the  
9 communications, meaning Meta acquires the contents of those communications while they are in  
10 transit. This is why Meta AI cannot function without internet connection turned on. Swedish  
11 journalists who revealed Meta's use of human contractors confirmed this real-time transmission by  
12 analyzing the network traffic generated when Meta AI was activated.

13 106. The transmission of audio, visual, and other data to Meta's servers demonstrates that  
14 Meta is able to access and process consumers' private content captured by Meta Smart Glasses in  
15 real time, notwithstanding Meta's representations that media captured on Meta Smart Glasses  
16 remains stored locally and under the consumer's control unless the user affirmatively chooses to  
17 share it.

18 107. Upon information and belief, Meta's interception and processing of consumers'  
19 private audio, video, and other data—beyond merely the queries or commands directed to Meta  
20 AI—occurred through the same real-time transmission process described above.

21 **E. Meta's Lack of Data Controls**

22 108. Particularly concerning is Meta's lack of controls relating to how data in its systems  
23 are used and processed, especially when it comes to AI and ML.

24 109. According to leaked internal Meta documents, one employee analogized Meta's lack  
25 of internal controls, and open (rather than closed) systems, to a lake: "You pour that ink [i.e., data]  
26  
27  
28

1 into a lake of water . . . at it flows . . . everywhere . . . How do you put that ink back in the bottle?  
2 How do you organize it again, such that it only flows to the allowed places in the lake?”<sup>55</sup>

3 110. In these same leaked documents, another employee explained Meta does “not have  
4 an adequate level of control and explainability over how our systems use data, and thus we can’t  
5 confidently make controlled policy changes or external commitments such as ‘we will not use X  
6 data for Y purpose.’ And yet, that is exactly what regulators expect us to do, increasing our risk of  
7 mistakes and misrepresentation.” Thus, once the data enters the Meta system, the data can be used  
8 for any and all purposes. Meta’s AI models, which are inherently a “black box”, are especially  
9 vulnerable to Meta’s inability to explain where data goes, how it is used, or to delete it.

10 111. Indeed, Meta’s own employees confirmed no one at Meta can state confidently where  
11 all the data about a user is stored and used. In a court hearing as part of the Cambridge Analytica  
12 scandal of 2018, Meta’s own engineers testified there was not a “single person” at Meta who could  
13 answer that question.

14 112. The private video and audio recordings Meta collected, disclosed, and used, as well  
15 as all annotations and models built off them, are treated the same way. Once this data enters Meta’s  
16 systems, there is no way to ensure it is ever deleted and all control over this data is gone.

17 **F. Plaintiffs and Class Members Do Not Consent to Defendants’ Conduct**

18 113. Plaintiffs and Class Members had no way of knowing that Defendants were  
19 collecting, using, and disclosing their private video and audio recordings.

20 114. Indeed, Meta consistently touted its products with privacy built in. Plaintiffs and  
21 Class Members would not expect this information would be intercepted, used, and disclosed without  
22 their consent.

23  
24  
25 \_\_\_\_\_  
26 <sup>55</sup> Lorenzo Franceschi-Bicchierai, *Facebook Doesn’t Know What It Does With Your Data, Or Where*  
27 *It Goes: Leaked Document*, VICE (Apr. 26, 2022), [https://www.vice.com/en/article/facebook-](https://www.vice.com/en/article/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes/)  
28 [doesnt-know-what-it-does-with-your-data-or-where-it-goes/](https://www.vice.com/en/article/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes/).

1 115. For example, none of this conduct is compatible with Meta’s recognition of its  
2 “responsibility to protect [consumers] privacy.”<sup>56</sup> Despite its representation that it has “teams  
3 dedicated to this work for everything [Meta] build[s]” including participating in the Partnership on  
4 AI’s Synthetic Media Framework and the White House’s voluntary commitments for AI, Meta  
5 lacked the “privacy safeguards” it promised consumers were already in place.<sup>57</sup>

6 116. Likewise, Meta represents that consumers are “in control of your data and content”  
7 and can “choose” what to “share with others, and when.” See **Figure 3**. Meta also promises that it  
8 provides “[e]asy to access settings” that let consumers “manage the information you share with  
9 Meta.”

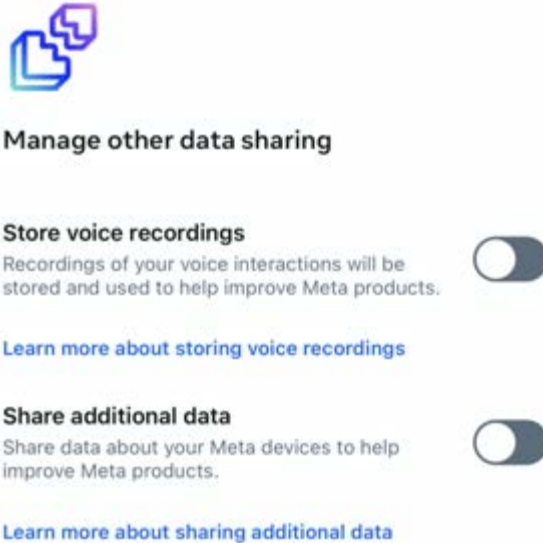
10 117. But Meta provides no way for consumers to opt-out of these practices, even if  
11 consumers did know about them. When consumers use Meta Smart Glasses, they need to download  
12 the “Meta View” mobile application, now rebranded as the “Meta AI” mobile application. Prior to  
13 April 2025, there were only two “privacy” settings that a consumer can toggle on or off in Meta  
14 View. See **Figure 6**.

15 118. As described in Figure 6, the only two settings were: (1) store voice recordings,  
16 which are “[r]ecordings of your voice interactions” (i.e., communications with Meta AI) and (2)  
17 share additional data, which are to “help improve Meta products.”

18  
19  
20  
21 \* \* \*

22  
23  
24  
25  
26 \_\_\_\_\_  
27 <sup>56</sup> Mike Clark, *Privacy Matters: Meta’s Generative AI Features*, *supra* n.27.

28 <sup>57</sup> *Id.*

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28**FIGURE 6**

119. Neither of these settings relate to the collection, use, or disclosure of consumers’ private videos and audio captured by the consumer. Indeed, Meta expressly notes that, even with “Additional Data” turned on, this “*does not include the photos and videos captured by your glasses.*”<sup>58</sup>

120. Moreover, the “voice recordings” and “interactions” stored and displayed to consumers in the Meta AI (previously the Meta View) app are *queries* the consumer posed directly to Meta AI (for example, “Hey Meta, what am I looking at?”). Both settings, and the voice interaction history displayed in the app, would lead a reasonable consumer to believe that Meta does not collect, use, or disclose private videos and audio captured by the consumer—it is only audio questions and commands they ask Meta AI directly.

121. Meta itself confirms this by representing in the Meta AI app (previously Meta View)

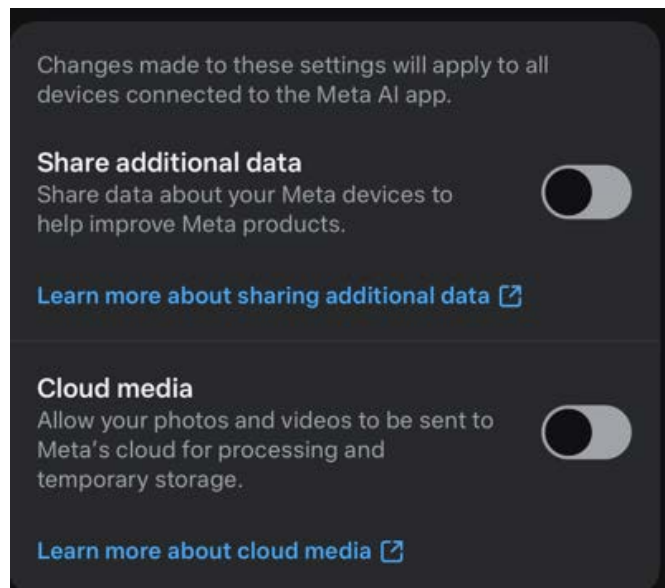
---

<sup>58</sup> META, *Control What Information You Share With Meta on Your AI Glasses and Wrist Devices*, <https://www.meta.com/help/ai-glasses/483508126732797/?srsltid=AfmBOorAL1XWkRMPTpyaNCpgc4NUAtNF2Kby9juK4K741FAQwDG9ZuQp> (last visited Mar. 13, 2026).

1 that “[v]oice interactions are *things you say while using the voice services* on Meta Wearable  
 2 Products, such as *voice controls*” including “things you say *when you use a wake-word* (for  
 3 example, if your AI Glasses are playing music, and you say ‘Hey Meta, pause the music’); when  
 4 you don’t use a wake-word for certain interactions (saying ‘pause music’ if your AI Glasses are  
 5 playing music, or ‘play message’ after we tell you that you have a new message)[.]” This clearly  
 6 does not include audio and video that is not directed to Meta AI via a prompt or command.

7 122. After April 2025, Meta changed these settings. In an email to consumers, Meta  
 8 stated that, going forward, Meta AI was always enabled unless a user manually turned off “Hey  
 9 Meta.” Additionally, consumers could no longer opt-out of whether voice recordings of “voice  
 10 interactions” with Meta AI were stored. Nevertheless, Meta still maintained the false promise that  
 11 consumers are “still in control.”

#### 12 FIGURE 7



23

24 123. Nowhere in this notice did Meta disclose that it would collect, use, or disclose  
 25 private video and audio recordings by default, nor did it disclose the content of these  
 26 communications would be used for AI training or shared with third parties. Meta also failed to  
 27

1 provide the option for consumers to opt-out.

2 124. Meta’s other representations when setting up Meta Smart Glasses further confirm  
3 that this conduct was not disclosed. For instance, on the page to “Learn more about Meta AI and  
4 your privacy” Meta explains “[h]ow [consumers] can control [their] data.” Meta confirmed that:

- 5 • “Meta AI” uses “what you say” to “*respond to your prompts*”
- 6 • That “[u]sing the camera with *Meta AI is optional*”
- 7 • Image data is only “processed” “*[w]hen you interact with Meta AI*”
- 8 • It is only “[i]mages *processed with AI*” and “voice transcripts” (i.e., user queries  
9 to Meta AI) that are “collected, used, and stored.”

10 “Meta AI captures voice and images *only when you interact with it.*”

11  
12  
13  
14  
15  
16  
17  
18 \* \* \*

**FIGURE 8**



**Learn more about Meta AI and your privacy**

Meta AI is a Large Language Model-driven conversational assistant that uses what you say and other data to respond to your prompts. [Learn more about Meta AI](#)

**Your voice transcript data**

If you enable and interact with Meta AI, your voice will be recorded, transcribed and processed as explained in our [privacy notice](#).

**Your image data**

When you interact with Meta AI, an image may be processed with AI on Meta's servers. Processing with AI includes the contents of your images like objects, points of interest and text. Meta AI may use this information to understand your location and provide you with a more relevant response. Using the camera with Meta AI is optional. [Learn more about how images are used](#).

**How your data is used**

Images processed with AI, voice transcripts, and related data will all be collected, used and stored according to Meta's [Privacy Policy](#), including to improve Meta products with help from trained reviewers and to train AI models. Your data may be shared with trusted partners to provide better responses.

**How you can control your data**

Meta AI captures voice and images only when you interact with it. You can turn off camera use, delete Meta AI interactions or disable Meta AI anytime in settings.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

125. In light of these claims, no reasonable consumer would believe that enabling Meta AI would mean Meta had free range over their private videos, audio and other data, including content they did not intend to capture or that does not relate to a Meta AI query. To the contrary, they would simply believe that the enablement of Meta AI was so the Meta Smart Glasses could effectively respond to the wake word “Hey Meta.” If Meta intended to do anything more than that, it should have stated as much, consistent with its promise for transparency and clear disclosures, which it did not live up to.

1 126. Accordingly, Plaintiffs and Class Members did not consent to Defendants' conduct,  
2 nor did they have any way to opt-out.

3 **G. Plaintiffs and Class Members have a Reasonable Expectation of Privacy in their**  
4 **User Data**

5 127. Plaintiffs and Class Members have a reasonable expectation of privacy in their  
6 private video and audio recordings, especially those revealing sensitive content.

7 128. Privacy polls and studies uniformly show that the overwhelming majority of  
8 Americans consider one of the most important privacy rights to be the need for an individual's  
9 affirmative consent before a company collects and shares its customers' personal data.

10 129. For example, a recent study by *Consumer Reports* shows that 92% of Americans  
11 believe that internet companies and websites should be required to obtain consent before selling or  
12 sharing consumers' data, and the same percentage believe internet companies and websites should  
13 be required to provide consumers with a complete list of the data that has been collected about them.  
14 Moreover, according to a study by *Pew Research Center*, a majority of Americans, approximately  
15 81%, are concerned about how companies use the data they collect about them.<sup>59</sup>

16 130. Users act consistent with these preferences. Following a new rollout of the iPhone  
17 operating software—which asks users for clear, affirmative consent before allowing companies to  
18 track users—85% of worldwide users and 94% of U.S. users chose not to share data when prompted.

19 131. Another recent study by DataGrail revealed that 67% of people were willing to pay  
20 \$100 or more annually to keep their information out of the hands of companies and the government.  
21 The same study revealed that 75% of people would abandon brands that do not take care of their  
22 data.<sup>60</sup>

23  
24 <sup>59</sup> Colleen McClain *et al.*, *How Americans View Data Privacy*, PEW RSCH. CTR. (Oct. 18, 2023),  
25 <https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/>.

26 <sup>60</sup> DATAGRAIL, *New DataGrail Research, The Great Privacy Awakening, Underscores How Far*  
27 *People are Willing to Go to Protect Their Personal Information in Absence of Federal Regulations*,  
28 <https://www.datagrail.io/press/new-datagrail-research-the-great-privacy-awakening/> (last visited  
Mar. 13, 2026).

1 132. With respect to Meta specifically, when it announced that it would begin using  
2 Facebook and Instagram users public posts to train its AI models, a post stating users did “not give  
3 Meta or anyone else permission” to use their data was shared hundreds of thousands of times.<sup>61</sup> This  
4 confirms consumers expect that Meta will not use their data, and certainly not their private videos  
5 and audio, to train its AI models.

6 133. Meta, in particular, was legally required to adhere to privacy expectations. Pursuant  
7 to a 2019 settlement with the Federal Trade Commission (“FTC”), Meta promised to review every  
8 new or modified product for risks to consumers’ privacy rights. Notably, however, an internal post  
9 provided to the *New York Times* from January 2025 suggests that Meta had “relaxed” this policy,  
10 despite the FTC agreement.<sup>62</sup> This further confirms the egregious nature of Meta’s conduct, and its  
11 invasion of consumers’ privacy rights.

12 134. Also notable, a German privacy watchdog—the Hamburg Data Protection Authority  
13 (“DPA”)—raised privacy concerns about these types of practices back in August 2019. Specifically,  
14 journalists had uncovered that Google was sharing audio recordings from its voice assistant with  
15 contractors for manual review to improve its speech technology. The Hamburg DPA criticized these  
16 practices as inconsistent with the General Data Protection Regulation (“GDPR”) and privacy  
17 expectations, noting there were “significant doubts” that the secret use of contractors to conduct a  
18 manual review of private audio recordings complied with this law.<sup>63</sup> Meta’s practices here are  
19 similar, if not worse.

20 135. Meta, as a direct competitor of Google, must have been aware of the scrutiny and  
21 privacy implications behind these practices. Nevertheless, it touted its (non-existent) privacy  
22

---

23 <sup>61</sup> Jesus Jimenez, *Worried About Meta Using Your Instagram to Train Its A.I.? Here’s What to Know*  
24 N.Y. TIMES (Sept. 26, 2024), <https://www.nytimes.com/article/meta-ai-scraping-policy.html>.

25 <sup>62</sup> Kashmir Hill *et al.*, *Meta Plans to Add Facial Recognition Technology to Its Smart Glasses*, N.Y.  
26 TIMES (Feb. 13, 2026), <https://www.nytimes.com/2026/02/13/technology/meta-facial-recognition-smart-glasses.html>.

27 <sup>63</sup> Natasha Lomas, *Google Ordered to Halt Human Review of Voice AI Recordings Over Privacy*  
28 *Risks*, TECHCRUNCH (Aug. 2, 2019), <https://techcrunch.com/2019/08/02/google-ordered-to-halt-human-review-of-voice-ai-recordings-over-privacy-risks/>.

1 controls and transparency all while engaging in the same conduct found to be privacy-invasive over  
2 six years ago.

3 136. Unsurprisingly, its conduct has drawn the same scrutiny. The United Kingdom’s  
4 Information Commissioner’s Office told *BBC News* that: “Service providers must clearly explain  
5 what data is collected and how it is used. The claims in this article are concerning. We will be writing  
6 to Meta to request information on how it is meeting its obligations under the U.K. data protection  
7 law.”<sup>64</sup>

8 137. Recent reports also suggest that seventeen countries have written to the European  
9 Commission over Meta’s privacy violations requesting further information on how it will address  
10 this conduct.<sup>65</sup>

#### 11 **H. Meta Profits from AI and ML Training**

12 138. As described above, Meta’s entire business model is generating revenue from  
13 advertising. Its AI ambitions are all centered around improving its ad targeting and delivery  
14 capabilities.

15 139. Meta has invested significantly in AI-based technology precisely to capitalize on  
16 how it can improve its revenue. As Mr. Zuckerberg stated, “We are now seeing a major AI  
17 acceleration. I expect 2026 to be a year where this wave accelerates even further.” Meta spent nearly  
18 \$72.2 billion in 2025 on AI investments, and plans to spend between \$115 billion and \$135 billion  
19 this year.<sup>66</sup>

---

20  
21  
22  
23  
24 <sup>64</sup> Chris Vallance, *Regulator contacts Meta over workers watching intimate AI glasses videos*, BBC  
NEWS (Mar. 4, 2026), <https://www.bbc.com/news/articles/c0q33nvj0qpo>.

25 <sup>65</sup> Graham Hope, *Euro Regulators Question Meta Over AI Glasses Privacy Fears*, AI BUSINESS  
26 (Mar. 5, 2026), <https://aibusiness.com/metaverse/euro-regulators-question-meta-over-ai-glasses-privacy-fears#close-modal>.

27 <sup>66</sup> Rithula Nisha, *Why Meta Plans to Double AI Investment as Profits Surge*, AI MAG. (Jan. 29,  
28 2026), <https://aimagazine.com/news/metasp-profit-surge-ai-spending-set-to-nearly-double>.

1 140. Data for AI training is particularly valuable. For instance, Google recently licensed  
2 content from Reddit to train its AI models for \$60 million a year.<sup>67</sup> Reddit represents that it made  
3 over \$200 million licensing this data to entities altogether.<sup>68</sup>

4 141. Stack Overflow and Shutterstock likewise charge AI companies to license its data.<sup>69</sup>  
5 Similarly, PhotoBucket has discussed with “multiple tech companies” licensing the photos and  
6 videos on its platform, with prices ranging from \$0.50-\$1.00 per photo and more than \$1 per video.

7 142. Meta’s use of consumers’ private video and audio recordings to improve its models’  
8 abilities to correctly detect certain images, conduct, or objects, directly improves Meta’s AI and  
9 ML-based offerings and its ultimate revenue.

#### 10 **I. Defendants Do Not Adhere to “Best Practices”**

11 143. Despite Meta’s promise that it adheres to “best practices and meets high standards  
12 for data protection”—it did not do so. This includes the very guidelines and principles it promised  
13 consumers it would adhere to.

14 144. For instance, Meta promises that it has “teams dedicated to this work for everything  
15 [Meta] build[s]” including participating in the Partnership on AI’s Synthetic Media Framework and  
16 the White House’s voluntary commitments for AI.<sup>70</sup> Its collection, use, and disclosure of consumers’  
17 private video and audio is inconsistent with the privacy principles enshrined in these frameworks  
18 and commitments.

19 145. For instance, the Partnership on AI’s Synthetic Media Framework (“PAI”) has a  
20 framework setting forth “responsible practices” (the “PAI Framework”). While Meta’s use of real

---

21 <sup>67</sup> Ann Tong, *et al.*, *Exclusive: Reddit in AI content licensing deal with Google*, REUTERS (Feb. 21,  
22 2024), <https://www.reuters.com/technology/reddit-ai-content-licensing-deal-with-google-sources-say-2024-02-22/>.

23 <sup>68</sup> Kyle Wiggers, *Reddit Says It’s Made \$203M So Far Licensing Its Data*, TECHCRUNCH (Feb. 22,  
24 2024), <https://techcrunch.com/2024/02/22/reddit-says-its-made-203m-so-far-licensing-its-data/>.

25 <sup>69</sup> Pares Dave, *Stack Overflow Will Charge AI Giants for Training Data*, WIRED (Apr. 20, 2023),  
<https://www.wired.com/story/stack-overflow-will-charge-ai-giants-for-training-data/>;  
26 SHUTTERSTOCK, *Shutterstock Builds on Data Licensing Strength with New AI Services for Model  
Training and Evaluation* (Oct. 7, 2025), <https://investor.shutterstock.com/news-releases/news-release-details/shutterstock-builds-data-licensing-strength-new-ai-services>.

27 <sup>70</sup> Mike Clark, *Privacy Matters: Meta’s Generative AI Features*, *supra* n.27.

1 consumers' private audio, video, and other data is not "synthetic media" the same principles apply.  
2 Section 2 of the PAI Framework expressly states to "[b]e transparent to users about tools and  
3 technologies' capabilities, functionality, limitations, and . . . potential risks." Meta was not  
4 transparent with consumers about its collection, use, and disclosure of their private data.

5 146. The White House's voluntary commitments for AI similarly emphasize privacy  
6 rights, including that companies joining this pledge commit to "advancing privacy" and "protecting  
7 privacy."<sup>71</sup> Meta did not protect consumers' privacy, it violated it.

8 147. Meta did not adhere to traditional best practices either. The most fundamental best  
9 practices for privacy are enshrined in the Fair Information Practice Principles ("FIPPs"), much of  
10 which form the foundation for the Federal Trade Commission's enforcement of fraudulent and  
11 unfair privacy-related business practices.<sup>72</sup>

12 148. The FIPPs first originated in a 1973 U.S. government report—the HEW Report  
13 published by the U.S. Department of Health, Education & Welfare—and has since been adopted by  
14 multiple agencies.<sup>73</sup>

15 149. Among these principles are: (1) a mandate that companies should clearly disclose  
16 what data is used, how it is used, and who it is shared with; (2) the need for companies to obtain  
17 consent to collect, use, or access data; (3) a prohibition on using information shared for one purpose  
18 for other undisclosed purposes; (4) a prohibition on using data for undisclosed purposes without  
19 obtaining additional consent; and (5) the idea of data minimization, which means that data should  
20 only be collected and stored for as long as necessary for the stated purpose.<sup>74</sup>

21  
22  
23 \_\_\_\_\_  
24 <sup>71</sup> THE WHITE HOUSE, *Voluntary AI Commitments* (Sept. 12, 2023),  
<https://www.whitehouse.gov/wp-content/uploads/2023/09/Voluntary-AI-Commitments-September-2023.pdf>.

25 <sup>72</sup> *Fair Information Practice Principles (FIPPs)*, <https://www.fpc.gov/resources/fipps/> (last visited  
26 Mar. 13, 2026).

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

28 <sup>74</sup> *Id.*

1 150. A 2012 FTC Report, titled *Protecting Consumer Privacy in an Era of Rapid Change*,  
2 also mirrors the FIPPs, calling for transparency, clear consumer disclosures and choice, as well as  
3 the concept of “privacy by design.”<sup>75</sup>

4 151. The National Institute of Standards and Technology uses a similar framework,  
5 expressly mirrored off the FIPPs, and the Organization for Economic Co-operation and  
6 Development (OECD) has adopted its own OECD Principles that closely mirror FIPPs.

7 152. Many of these best practices have also been codified into law, including in the GDPR  
8 and California Consumer Privacy Act (“CCPA”).

9 153. Meta, as well as the other Defendants, did not adhere to these best practices. To the  
10 contrary, Meta represented the Meta Smart Glasses—which it developed with Luxottica—as  
11 consistent with privacy standards and best practices, including allowing consumer choice and  
12 transparency. But this was false. Meta did not disclose that it would collect, use, and disclose  
13 consumers’ private video and audio content, nor did it provide consumers with any choice in the  
14 matter.

15 154. Finally, Meta did not adhere to “best practices” specific to the AI industry either.  
16 Both OpenAI and Anthropic—two of Meta’s AI competitors—provide the ability for consumers to  
17 opt-out of having their inputs used to train AI models. Industry practice increasingly favors either  
18 obtaining express user consent before using user inputs—including uploaded images, videos, or  
19 text—for model training, providing an opt-out right, or refraining from using such data altogether.  
20 Meta adopted none of these practices, but continued to represent it adhered to privacy expectations,  
21 high standards, and industry best practices.

22 155. For these reasons, Meta’s claim that it adheres to best practices are categorically  
23 false. As are its claims that it consulted with “regulators, policymakers, and experts”—none of  
24 whom ever would have endorsed or approved of its conduct.

---

25 <sup>75</sup> *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and*  
26 *Policymakers*, FED. TRADE COMM’N (Mar. 2012),  
27 <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

**TOLLING**

1  
2 156. The applicable statutes of limitation have been tolled as a result of Defendants’  
3 knowing and active concealment and denial of the facts alleged herein.

4 157. Defendants’ knowing and active concealment and denial of the facts alleged herein  
5 toll any applicable statute(s) of limitations. Plaintiffs and Class Members could not reasonably have  
6 discovered the true nature and extent of Meta’s collection, transmission, storage, and use of data  
7 captured through the Meta Smart Glasses until the facts alleged herein became known.

8 158. Plaintiffs and Class Members had no reasonable ability to discover, within the  
9 applicable statute of limitations, that Defendants were misrepresenting the privacy protections, data  
10 practices, and safeguards of the Meta Smart Glasses, and could not have discovered through the  
11 exercise of reasonable diligence that Defendants were concealing such information and  
12 misrepresenting the features, capabilities, privacy controls, reliability, functionality, characteristics,  
13 and performance of the Meta Smart Glasses. Plaintiffs only learned of this conduct shortly before  
14 the filing of this complaint.

15 159. Any statutes of limitation otherwise applicable to any claims asserted herein thus  
16 have been tolled by the discovery rule.

17 160. All applicable statutes of limitations have also been tolled by Defendants’ knowing,  
18 active, and ongoing fraudulent concealment of the material facts alleged herein.

19 161. Defendants had a duty to disclose, among other things, the true scope and nature of  
20 the data collection, transmission, retention, and use practices associated with the Meta Smart  
21 Glasses, because such practices are central to the privacy and functionality of the product and were  
22 the subject of Defendants’ own affirmative marketing representations.

23 162. Despite their knowledge, Defendants actively concealed these material facts from  
24 Plaintiffs and Class Members while continuing to profit from the sale of the Meta Smart Glasses  
25 they marketed as a product “designed for privacy, controlled by you.”

26 163. As a result of Defendants’ active concealment, any and all applicable statutes of  
27 limitations otherwise applicable to the allegations herein have been tolled.

1 164. Defendants had a duty to disclose to Plaintiffs and Class Members the true character,  
2 nature, and quality of the Meta Smart Glasses, including the fact that the glasses transmit consumer  
3 and bystander data to Meta's cloud servers and third party contractors for analysis and AI model  
4 training and that the privacy protections Meta marketed were false.

5 165. Instead, Defendants concealed the true character, nature, and quality of the Meta  
6 Smart Glasses and knowingly made misrepresentations about the privacy protections, data practices,  
7 reliability, functionality, characteristics, and performance of the Meta Smart Glasses.

### 8 CLASS ACTION ALLEGATIONS

9 166. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23  
10 individually and on behalf of the following Classes:

11 **Nationwide Class:** All persons who purchased Meta Smart Glasses in the United  
12 States or its Territories, or who otherwise used or were captured by Meta Smart  
13 Glasses.<sup>76</sup>

14 **Purchaser Subclass:** All persons who purchased Meta Smart Glasses in the United  
15 States or its Territories.

16 167. Excluded from the Classes are: (1) any Judge or Magistrate presiding over this action  
17 and any members of their immediate families; (2) the Defendants, Defendants' subsidiaries,  
18 affiliates, parents, successors, predecessors, and any entity in which the Defendants or their parents  
19 have a controlling interest and their current or former employees, officers, and directors; and  
20 (3) Plaintiffs' counsel and Defendants' counsel.

21 168. **Numerosity:** The exact number of members of the Classes is unknown and  
22 unavailable to Plaintiffs at this time, but individual joinder in this case is impracticable. The Classes  
23 likely consists of millions of individuals, and the members can be identified through Defendants'  
24 records.

---

25  
26 <sup>76</sup> To extent the Court finds California law does not apply to all Class Members, Plaintiffs reserve  
27 the right to bring claims on behalf of a California Subclass consisting of all individuals in California  
28 who purchased Meta Smart Glasses or who otherwise used or were captured by Meta Smart Glasses.

1           169.   **Predominant Common Questions:** The Classes' claims present common questions  
2 of law and fact, and those questions predominate over any questions that may affect individual Class  
3 Members. Common questions for the Classes include, but are not limited to, the following:

- 4           •       Whether Defendants violated Plaintiffs' and Class Members' privacy rights;
- 5           •       Whether Defendants' acts and practices violated common law invasion of  
6           privacy;
- 7           •       Whether Defendants were unjustly enriched;
- 8           •       Whether Defendants' acts and practices violated the California Invasion of  
9           Privacy Act, Cal. Penal Code §§ 630, *et seq.*;
- 10          •       Whether Plaintiffs and the Class Members are entitled to equitable relief,  
11          including but not limited to, injunctive relief, restitution, and disgorgement; and
- 12          •       Whether Plaintiffs and the Class Members are entitled to actual, statutory,  
13          punitive or other forms of damages, and other monetary relief.

14           170.   **Typicality:** Plaintiffs' claims are typical of the claims of the other members of the  
15 Classes. The claims of Plaintiffs and the members of the Classes arise from the same conduct by  
16 Defendants and are based on the same legal theories.

17           171.   **Adequate Representation:** Plaintiffs have and will continue to fairly and adequately  
18 represent and protect the interests of the Classes. Plaintiffs have retained counsel competent and  
19 experienced in complex litigation and class actions, including litigations to remedy privacy  
20 violations. Plaintiffs have no interests that are antagonistic to the interests of the Classes, and  
21 Defendants have no defenses unique to any Plaintiff. Plaintiffs and their counsel are committed to  
22 vigorously prosecuting this action on behalf of the members of the Classes, and they have the  
23 resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to the interests of  
24 the other members of the Classes.

25           172.   **Substantial Benefits:** This class action is appropriate for certification because class  
26 proceedings are superior to other available methods for the fair and efficient adjudication of this  
27 controversy and joinder of all members of the Classes is impracticable. This proposed class action  
28

1 presents fewer management difficulties than individual litigation, and provides the benefits of single  
2 adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment  
3 will create economies of time, effort, and expense and promote uniform decision-making.

4 173. Plaintiffs reserve the right to revise the foregoing class allegations and definitions  
5 based on facts learned and legal developments following additional investigation, discovery, or  
6 otherwise.

7 **CALIFORNIA LAW APPLIES TO ALL CLASSES & CLAIMS**

8 174. California substantive laws apply to every member of the Classes. California's  
9 substantive laws may be constitutionally applied to the claims of Plaintiffs and the Classes under  
10 the Due Process Clause, 14th Amend. § 1, and the Full Faith and Credit Clause, Art. IV. § 1 of the  
11 U.S. Constitution. California has significant contact, or significant aggregation of contacts, to the  
12 claims asserted by Plaintiffs and Class Members, thereby creating state interests to ensure that the  
13 choice of California state law is not arbitrary or unfair.

14 175. Meta and Sama maintain their principal places of business in California and conduct  
15 substantial business in California, such that California has an interest in regulating Meta's and  
16 Sama's conduct under its laws. Meta and Sama also selected California law as the law to govern all  
17 disputes with their customers in their terms of service. Meta and Sama's decision to reside in  
18 California and avail themselves of California's laws, renders the application of California law to the  
19 claims herein constitutionally permissible.

20 176. The application of California laws to the Classes is also appropriate under  
21 California's choice of law rules because California has significant contacts to the claims of Plaintiffs  
22 and the proposed Classes, and California has a greater interest in applying its laws here given Meta  
23 and Sama's locations and the location of the conduct at issue than any other interested state.

24  
25  
26 \* \* \*

**CLAIMS FOR RELIEF**

**FIRST CLAIM FOR RELIEF**

**Violation of Common Law Invasion of Privacy – Intrusion Upon Seclusion  
(On Behalf of the Plaintiffs and the Nationwide Class)  
(Against All Defendants)**

177. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

178. A plaintiff asserting claims for intrusion upon seclusion must plead (1) that the defendant intentionally intruded into a place, conversation, or matter as to which Plaintiffs have a reasonable expectation of privacy; and (2) that the intrusion was highly offensive to a reasonable person.

179. Plaintiffs and Class Members have a reasonable expectation of privacy in their video, audio, and other personal data. Plaintiffs and Class Members reasonably expected this information would remain private and confidential and would not be collected or disclosed to third parties without their consent.

180. Likewise, Plaintiffs and Class Members have a reasonable expectation of privacy that their private video, audio, and other personal data would not be used without their knowledge or consent and particularly not to train AI modeling by one of the largest advertising companies in the world.

181. This expectation of privacy is especially heightened given Defendants’ consistent representations to users that this information would be safeguarded and that consumers had control over which information was shared and used

182. For instance, with respect to Meta AI and Meta AI-powered products, Meta represented that it would ensure “that people understand the types of data we use to train the models that power our generative AI products.”<sup>77</sup> It also assured users that it built “important privacy safeguards” and that each of its “generative AI features go through a rigorous internal privacy review” to “ensure [Meta is] using people’s data responsibly.”<sup>78</sup>

---

<sup>77</sup> Meta, *Building Generative AI Features Responsibly*, *supra* n.4.

<sup>78</sup> Mike Clark, *Privacy Matters: Meta’s Generative AI Features*, *supra* n.27.

1 183. Meta also represented that consumers are “in control of [their] data and content” and  
2 can “choose” what to “share with others, and when.” *See* Figure 3. Meta promises that it provides  
3 “[e]asy to access settings” that let consumers “manage the information you share with Meta.”

4 184. Given these representations, and the nature of the data Defendants received,  
5 Plaintiffs and Class Members had a reasonable expectation of privacy in their confidential and  
6 private video, audio, and other interactions using Meta Smart Glasses and expected this information  
7 would not be disclosed or used to train AI models.

8 185. Meta’s collection and disclosure of Plaintiffs’ and Class Members’ confidential and  
9 private videos, audio, and other interactions to third parties like Sama constitutes an intentional  
10 intrusion upon Plaintiffs’ and Class Members’ solitude or seclusion. This is true for videos Plaintiffs  
11 intended to capture using their Meta Smart Glasses, as well as those that were recorded without their  
12 knowledge or consent.

13 186. Meta’s use of Plaintiffs’ and Class Members’ confidential and private videos, audio,  
14 and other interactions—as well as annotated versions of this data—to train AI models also  
15 constitutes an intentional intrusion upon Plaintiffs’ and Class Members’ solitude or seclusion.

16 187. Sama’s receipt, review, and annotation of Plaintiffs’ and Class Members’  
17 confidential and private videos, audio, and other interactions, pursuant to its agreement with Meta,  
18 is likewise an intentional intrusion upon Plaintiffs’ and Class Members’ solitude or seclusion.  
19 Indeed, as noted by Sama’s own contractors, the videos they reviewed make them feel as if they  
20 were looking straight into other people’s “private li[v]e[s].”

21 188. Luxottica’s offering for sale of Meta Smart Glasses that were equipped with, and did  
22 in fact, result in the unlawful collection, disclosure, and use of Plaintiffs’ and Class Members’  
23 confidential and private videos, audio, and other interactions also violated Plaintiffs’ and Class  
24 Members’ reasonable expectation of privacy, is highly offensive, and violated Plaintiffs’ and Class  
25 Members’ solitude or seclusion.

26 189. The surreptitious disclosure and use of confidential and private data from millions of  
27 individuals was highly offensive because it violated expectations of privacy that have been  
28

1 established by social norms. Privacy polls and studies show that the overwhelming majority of  
2 Americans believe one of the most important privacy rights is the need for an individual's  
3 affirmative consent before personal data is collected or shared.

4 190. The offensiveness of this conduct is all the more apparent because Defendants'  
5 disclosure of this information was conducted in secret in a manner that Plaintiffs and Class Members  
6 would be unable to detect. And it was contrary to the actual representations made by Meta and  
7 Luxottica, including in promotional materials for the Meta Smart Glasses offered by Meta and  
8 Luxottica.

9 191. Training AI models using data without consent is particularly egregious, and against  
10 privacy expectations, because of the opaque nature of AI models. Once data is incorporated into  
11 these models, it becomes extraordinarily difficult, if not practically impossible, to identify, isolate,  
12 or remove because of their "black box" nature. Meaning, individuals have no meaningful ability to  
13 ever reclaim control over their personal information.

14 192. Plaintiffs and Class Members did not consent to, authorize, or know about  
15 Defendants' intrusion at time it occurred. Accordingly, Plaintiffs and Class Members never agreed  
16 that Defendants could disclose their data to third parties. Indeed, Meta promised the opposite. In  
17 2024, a Meta spokesperson represented to *TechCrunch* that "photos and videos captured on Ray-  
18 Ban Meta are *not* used by Meta for training as long as the user doesn't submit them to AI." Meaning,  
19 so long as consumers do not ask Meta AI to analyze, view, or interpret their recordings or what they  
20 are currently viewing through their Meta Smart Glasses.

21 193. As a result of Defendants' actions, Plaintiffs and Class Members have suffered harm  
22 and injury, including but not limited to an invasion of their privacy rights.

23 194. Plaintiffs and Class Members have been damaged as a direct and proximate result of  
24 Defendants' privacy invasions and are entitled to just compensation, including monetary damages.  
25 Plaintiffs and Class Members seek all appropriate relief for that injury, including but not limited to  
26 damages and all other relief that may be just or proper.

1 195. Plaintiffs and Class Members are also entitled to punitive damages resulting from the  
2 malicious, willful, and intentional nature of Defendants’ actions, directed at injuring Plaintiffs and  
3 Class Members in conscious disregard of their rights. Such damages are needed to deter Defendants  
4 from engaging in such conduct in the future.

5 **SECOND CLAIM FOR RELIEF**  
6 **Violation of Article I, Section 1 of the California Constitution (Invasion of Privacy)**  
7 **(On Behalf of Plaintiffs and the Nationwide Class)**  
8 **(Against All Defendants)**

9 196. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with  
10 the same force and effect as if fully restated herein.

11 197. Article I, Section 1 of the California Constitution provides: “All people are by nature  
12 free and independent and have inalienable rights. Among these are enjoying and defending life and  
13 liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety,  
14 happiness, and privacy.” California Constitution, Article I, Section 1.

15 198. To state a claim for invasion of privacy under the California Constitution, a plaintiff  
16 must establish (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and  
17 (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an  
18 egregious breach of the social norms.

19 199. The right to privacy in California’s Constitution creates a right of action against  
20 private and government entities.

21 200. Plaintiffs and Class Members have and continue to have a reasonable expectation of  
22 privacy in their personal information, identities, and private data, pursuant to Article I, Section I of  
23 the California Constitution.

24 201. The video, audio, and other private communications that Defendants intercepted,  
25 collected, used, and disclosed without Plaintiffs’ and Class Members’ consent defeated established  
26 privacy-mechanisms, social norms, and expectations of privacy. These acts were also inconsistent  
27 with Meta’s own representations, including its privacy promises and representation that only Meta  
28 AI queries would be collected, used, and processed for AI training.



1 the contents of any the above communications knowing or having reason to know the information  
2 was obtained through an interception of a wire, oral, or electronic communication.<sup>79</sup>

3 208. Accordingly, the ECPA prohibits the interception, use, and disclosure of the content  
4 of the above communications.

5 209. The ECPA provides a private right of action to any person whose electronic  
6 communications are intercepted. 18 U.S.C. § 2520(a).

7 210. The Meta Smart Glasses, and Plaintiffs’ other devices, constitute “devices” within  
8 the meaning of 18 U.S.C. § 2510(5).

9 211. Meta violated the ECPA because it intentionally intercepted Plaintiffs’ and Class  
10 Members’ private video, audio, and other personal communications, which fall within the ECPA’s  
11 definition of wire, oral, and electronic communications.

12 212. Meta also violated the ECPA because it used, endeavored to use, and procured others  
13 to use Plaintiffs’ and Class Members’ oral communications, which were transmitted through a  
14 device that transmits signals over a wire, line, or cable. The use of these communications occurred  
15 at locations operated by Sama and Meta, which are businesses that transact in interstate and foreign  
16 commerce and—when used by Meta—this use occurred within the United States.

17 213. Meta further violated the ECPA by intentionally disclosing and endeavoring to  
18 disclose the content of Plaintiffs’ and Class Members’ private video, audio, and other personal  
19 communications to third parties, including Sama.

20 214. And Meta violated the ECPA by intentionally using, and endeavoring to use, the  
21 content of Plaintiffs’ and Class Members’ private video, audio, and other personal communications,  
22 including to train AI models.

23 215. Sama violated the ECPA because, among other things, it intentionally aided, agreed,  
24 and conspired with Meta to procure these protected communications and the content thereof.

25  
26 \_\_\_\_\_  
27 <sup>79</sup> The ECPA lists other circumstances where such use or endeavor to use violate the ECPA but are  
28 not listed here for brevity.

1           216. Sama also violated the ECPA because it used and endeavored to use Plaintiffs' and  
2 Class Members' oral communications to annotate and label them on Meta's behalf, which were  
3 obtained through a device that transmits signals over a wire, line, and cable. These communications  
4 were used at locations operated by Sama, which is a business that transacts in interstate and foreign  
5 commerce.

6           217. Sama again violated the ECPA by using and endeavoring to use the content of  
7 Plaintiffs' and Class Members' private video, audio, and other personal communications. As Sama's  
8 own contractors have confirmed, they review the substance of these audio and video recordings,  
9 which constitute content.

10           218. Luxottica violated the ECPA because it intentionally procured, and permitted Meta,  
11 to intercept, use, and disclose Plaintiffs' and Class Members' private video, audio, and other  
12 personal communications, and the content thereof, by embedding Meta's technology in glasses sold  
13 and offered by Luxottica.

14           219. In engaging in the above conduct, Defendants acted with a tortious and criminal  
15 purpose, and intended to violate state and federal constitutional and statutory provisions, including:

- 16           • A knowing intrusion upon Plaintiffs' and Class Members' seclusion;
- 17           • The intentional disclosure of private facts;
- 18           • Violation of the California Invasion of Privacy Act ("CIPA");
- 19           • Violation of various state consumer protection statutes, including but not limited  
20 to the Unfair Competition Law ("UCL"); and
- 21           • Violation of various state computer privacy and property statutes, including but  
22 not limited to the California Comprehensive Computer Data Access and Fraud  
23 Act ("CDAFA"), Cal. Penal Code § 502.

24           220. The unauthorized collection, disclosure, and use of private communications—and  
25 endeavoring and procuring others to do so—for profit is tortious in and of itself. Meta, in particular,  
26 collected, disclosed, and used these communications with knowledge that it represented these  
27 communications would remain private, but put its desire and purpose of maximizing its own profits  
28

1 above the needs, expectations, and privacy rights of Plaintiffs and Class Members. Thus, Meta’s  
2 conduct was especially tortious.

3 221. Both Sama and Meta continued to commit the violations described herein, despite  
4 creating or receiving annotations that (at a minimum) revealed the private nature of these video,  
5 audio, and other communications. Thus, neither Sama nor Meta can claim ignorance, or that they  
6 did not know, or the tortious and criminal nature of their own acts.

7 222. Plaintiffs and Class Members seek all available relief for these violations, including  
8 statutory damages, punitive damages in an amount to be determined by a jury, and reasonable  
9 attorneys’ fee and other litigation costs reasonably incurred pursuant to 18 U.S.C § 2520.

10 **FOURTH CLAIM FOR RELIEF**  
11 **Violation of the California Invasion of Privacy Act (“CIPA”)**  
12 **Cal. Penal Code § 631**  
13 **(On Behalf of Plaintiffs and the Nationwide Class)**  
14 **(Against All Defendants)**

15 223. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with  
16 the same force and effect as if fully restated herein.

17 224. The California Legislature enacted the California Invasion of Privacy Act, Cal. Penal  
18 Code §§ 630, *et seq.* (“CIPA”) finding that “advances in science and technology have led to the  
19 development of new devices and techniques for the purpose of eavesdropping upon private  
20 communications and that the invasion of privacy resulting from the continual and increasing use of  
21 such devices and techniques has created a serious threat to the free exercise of personal liberties and  
22 cannot be tolerated in a free and civilized society.” *Id.* § 630. Thus, the intent behind CIPA is “to  
23 protect the right of privacy of the people of this state.” *Id.*

24 225. Cal. Penal Code § 631 imposes liability on any person who “by means of any  
25 machine, instrument, contrivance, or in any other manner” (1) “intentionally taps, or makes any  
26 unauthorized connection . . . with any telegraph or telephone wire, line, cable, or instrument,” (2)  
27 “willfully and without the consent of all parties to the communication, or in any unauthorized  
28 manner, reads or attempts to read, or to learn the contents or meaning of any message, report, or

1 communication while the same is in transit or passing over any wire, line, or cable, or is being sent  
2 from, or received at any place within [the state of California],” (3) “uses, or attempts to use, in any  
3 manner, or for any purpose, or to communicate in any way, any information so obtained,” or (4)  
4 “aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or  
5 cause to be done any of the acts or things mentioned above in this section.”

6 226. Defendants are persons for purposes of § 631.

7 227. Meta maintains its principal place of business in California, where it designed,  
8 contrived, agreed, conspired, effectuated, and received the interception, and used the contents of  
9 Plaintiffs and Class Members’ communications. Additionally, Meta has adopted California  
10 substantive law to govern its relationship with users, and its interception of, at least, the content of  
11 Plaintiffs’ and California Class Members’ communications occurred from their location and  
12 residence in California.

13 228. Sama maintains its principal place of business in California, where it designed,  
14 contrived, agreed, conspired, effectuated, and/or received the contents of Plaintiffs and Class  
15 Members’ communications. This includes entering into a contractual agreement with Meta, located  
16 in California, to process and annotate the content of intercepted communications. Additionally,  
17 Sama has adopted California substantive law in its respective Terms of Use.

18 229. While Luxottica does not maintain its principal place of business in California, it  
19 designed, contrived, agreed, enabled, and conspired with, at least, Meta in California, to offer the  
20 Meta Smart Glasses with its wiretapping functionality to intercept the contents of Plaintiffs and  
21 Class Members’ communications.

22 230. Meta Smart Glasses, and Plaintiffs’ and Class Members’ devices, are a “machine,  
23 instrument, contrivance, or . . . other manner.”

24 231. At all relevant times, Meta, through the Meta Smart Glasses, intentionally tapped or  
25 made unauthorized connections with the lines of internet communication utilized by Plaintiffs and  
26 Class Members without the consent of all parties to the communication.

1           232. Meta, willfully and without the consent of Plaintiffs and Class Members, read or  
2 attempt to read, or learn the contents or meaning of Plaintiffs' and Class Members' communications  
3 while the communications are in transit or passing over any wire, line or cable, or were being  
4 received at any place within California, when it intercepted Plaintiffs' and Class Members'  
5 communications and data in real time.

6           233. Meta and Sama used or attempted to use the content of the communications  
7 intercepted through the Meta Smart Glasses, including to train AI models. This includes annotating,  
8 labeling, and/or immediately processing the content obtained through Meta Smart Glasses,  
9 including videos and audio.

10           234. At all relevant times, Luxottica and Sama aided, employed, agreed with, and  
11 conspired with Meta to intercept and use Plaintiffs' and Class Members' private communications.  
12 These communications were transmitted to, processed, and intercepted by Meta in real time.

13           235. The interception of Plaintiffs' and Class Members' communications was without  
14 authorization and consent from the Plaintiffs and Class Members. Accordingly, the interception was  
15 unlawful and tortious.

16           236. Plaintiffs and the Class Members seek statutory damages in accordance with  
17 § 637.2(a), which provides for the greater of: (1) \$5,000 per violation; or (2) three times the amount  
18 of damages sustained by Plaintiffs and the Classes in an amount to be proven at trial, as well as  
19 injunctive or other equitable relief that may be proper.

20           237. Plaintiffs and Class Members have also suffered irreparable injury from these  
21 unauthorized acts. Plaintiffs' and Class Members' confidential and private data has been collected,  
22 viewed, accessed, used, and stored by Defendants, and has not been destroyed. Due to the continuing  
23 threat of such injury, Plaintiffs and Class Members have no adequate remedy at law, and therefore,  
24 Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief.

25  
26  
27  
28

\* \* \*

**FIFTH CLAIM FOR RELIEF**  
**Violation of CIPA**  
**Cal. Penal Code § 632**  
**(On Behalf of Plaintiffs and the Nationwide Class)**  
**(Against Meta)**

1  
2  
3  
4 238. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with  
5 the same force and effect as if fully restated herein.

6 239. Cal. Penal Code § 632 prohibits “intentionally and without the consent of all parties  
7 to a confidential communication,” using “an electronic amplifying or recording device to eavesdrop  
8 upon or record the confidential communication.”

9 240. Meta Smart Glasses, and Plaintiffs’ devices, are electronic amplifying or recording  
10 devices for purposes of § 632.

11 241. Section 632 defines “confidential communication” as “any communication carried  
12 on in circumstances as may reasonably indicate that any party to the communication desires it to be  
13 confined to the parties thereto[.]”

14 242. Plaintiffs’ and Class Members’ communications were confidential communications  
15 for purposes of § 632, including because Plaintiffs and Class Members had an objectively reasonable  
16 expectation of privacy that their private videos, audio, and other data would not be collected,  
17 intercepted, shared, or used.

18 243. Plaintiffs and Class Members expected their communications to be confined to their  
19 local devices, rather than intercepted and used by Meta or others, because of Meta’s consistent  
20 representations that these communications would remain confidential. Plaintiffs and Class Members  
21 did not expect Meta to secretly eavesdrop upon or record this information and their communications.

22 244. By contemporaneously intercepting and recording Plaintiffs’ and Class Members’  
23 confidential communications through this technology, Meta eavesdropped and/or recorded  
24 confidential communications through an electronic amplifying or recording device in violation of §  
25 632 of CIPA.



1           251. Plaintiffs’ and Class Members’ devices, including smart phones and Meta Smart  
2 Glasses, constitute “[c]omputer systems” within the meaning of the CDAFA. *Id.* § 502(b)(5). The  
3 functionality of these devices constitute “[c]omputer services” within the meaning of the CDAFA.  
4 *Id.* § 502(b)(4).

5           252. The data that Meta and Sama accessed, used, and/or disclosed from Plaintiffs’ and  
6 Class Members’ devices constitute “[d]ata” within the meaning of the CDAFA. *Id.* § 502(b)(8)  
7 (defining data to mean “a representation of information, knowledge, facts, concepts, computer  
8 software, computer programs or instructions. Data may be in any form, in storage media, or as stored  
9 in the memory of the computer or in transit or presented on a display device.”).

10           253. Meta violated § 502(c)(1) of the CDAFA by knowingly accessing, without  
11 permission, Plaintiffs’ and Class Members’ devices in order to wrongfully obtain, control, and use  
12 their personal data in violation of users’ reasonable expectations of privacy.

13           254. Meta and Sama violated § 502(c)(2) of the CDAFA by knowingly and without  
14 permission taking, copying, and making use of Plaintiffs’ and the Class Members’ personal data,  
15 which came from their devices.

16           255. Meta violated § 502(c)(3) by knowingly and without permission causing the  
17 functionality of Plaintiffs’ and Class Members’ devices to be used for the purposes of obtaining,  
18 taking, copying, and using Plaintiffs’ and Class Members’ personal data.

19           256. Meta violated § 502(c)(7) by knowingly and without permission accessing Plaintiffs’  
20 devices, and the functionality thereof.

21           257. Luxottica violated § 502(c)(6) by knowingly and without permission providing the  
22 means to, and assisting Meta in, accessing Plaintiffs’ devices and the functionality thereof.

23           258. Under § 502(b)(12) of the CDAFA a “Computer contaminant” is defined as “any set  
24 of computer instructions that are designed to . . . record, or transmit information within a computer,  
25 computer system, or computer network without the intent or permission of the owner of the  
26 information.”

1           259. Meta’s technology constitutes a “computer contaminant” because it instructed  
2 Plaintiffs’ devices and their functionality to record and transmit information and data to Meta  
3 without their permission or consent. Plaintiffs and Class Members had no way of knowing,  
4 removing, or opting out of this practice.

5           260. Plaintiffs and Class Members suffered damage and loss as a result of Defendants’  
6 conduct. Defendants’ practices have deprived Plaintiffs and the Class Members of control over their  
7 valuable property (namely, their private data), the ability to receive compensation for that data, and  
8 the ability to withhold their data for sale. Defendants’ practices have violated Plaintiffs’ and Class  
9 Members’ private interests by collecting, disclosing, and using their private data.

10           261. Plaintiffs and Class Members who purchased their Meta Smart Glasses also suffered  
11 a quantifiable loss because they expended sums on a product worth considerably less in light of its  
12 privacy invasive nature.

13           262. Plaintiffs and Class Members also suffered harm because Defendants unjustly  
14 profited from this conduct, including unjust gains earned by selling Meta Smart Glasses, and from  
15 the private data used for (at least) Meta and Sama’s own business purposes for profit.

16           263. Plaintiffs and Class Members seek compensatory damages in accordance with  
17 CDAFA § 502(e)(1), in an amount to be proven at trial, and injunctive or other equitable relief.

18           264. Plaintiffs and the Class Members are entitled to punitive or exemplary damages  
19 pursuant to Cal. Penal Code § 502(e)(4) because Defendants’ violations were willful and, upon  
20 information and belief, Defendants are guilty of oppression, fraud, or malice as defined in Cal. Civil  
21 Code § 3294. Plaintiffs and Class Members are also entitled to recover their reasonable attorneys’  
22 fees under § 502(e)(2).

23  
24  
25  
26  
27  
28

\* \* \*

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**SEVENTH CLAIM FOR RELIEF**  
**Unfair Competition Law (“UCL”)**  
**Cal. Bus. & Prof. Code §§ 17200 *et seq.***  
**(On Behalf of Plaintiffs and the Nationwide Class)**  
**(Against All Defendants)**

265. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

266. The UCL prohibits any “unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue, or misleading advertising.” Cal. Bus. & Prof. Code § 17200.

267. Defendants are “person[s]” as defined by Cal. Bus. & Prof. Code § 17201.

268. Defendants violated the UCL by engaging in fraudulent, unlawful, and unfair business acts and practices.

269. Meta engaged in fraudulent business acts and practices because it repeatedly represented that it would, among other things, fully disclose how it trains AI models, that consumers could limit what data it obtained and used through Meta Smart Glasses, and that only limited data was sent to and processed by Meta and its systems. Meta made these representations on its website, in the Meta Smart Glasses account set-up, and elsewhere.

270. Further, Meta did not disclose that it collects, uses, and shares consumers’ private audio and video with others, which is material information that Meta had a duty to disclose.

271. Defendants’ “unlawful” acts and practices include its violation of the ECPA, CIPA, CDAFA, the common law right of privacy, and each of the other laws described herein.

272. Defendants’ conduct violated the spirit and letter of these laws, which protect property and privacy interests and prohibit the unauthorized collection, use, and disclosure of private communications.

273. Defendants’ “unfair” acts and practices include their (1) sale of a product with inherently privacy-invasive functionality that was hidden to ordinary consumers; and/or (2) the surreptitious interception, collection, use, and/or disclosure of private communications without consent.

1           274. Plaintiffs and Class Members were completely unaware of Defendants’ conduct and  
2 could not have anticipated Defendants’ intrusion into their privacy through their fraudulent,  
3 unlawful, and/or unfair practices. Accordingly, Plaintiffs and Class Members could not avoid the  
4 harm Defendants caused.

5           275. Defendants’ conduct was immoral, unethical, oppressive, unscrupulous and  
6 substantially injurious to Plaintiffs and Class Members. Further, the gravity of the harm of  
7 Defendants’ secret collection, disclosure, and use of Plaintiffs’ and Class Members’ private  
8 communications is significant, and there is no corresponding benefit resulting from such conduct.

9           276. Plaintiffs and Class Members suffered injury, damage, and loss as a result of  
10 Defendants’ conduct. Defendants’ practices have deprived Plaintiffs and the Class Members of  
11 control over their valuable property (namely, their private data), the ability to receive compensation  
12 for that data, and the ability to withhold their data for sale. Defendants’ practices have violated  
13 Plaintiffs’ and Class Members’ private interests by collecting, disclosing, and using their private  
14 data.

15           277. Plaintiffs and Class Members who purchased their Meta Smart Glasses also suffered  
16 a quantifiable loss and harm because they expended sums on a product worth considerably less in  
17 light of its privacy invasive nature.

18           278. Defendants unjustly profited from this conduct, including unjust gains earned by  
19 selling Meta Smart Glasses, and from the private data used for (at least) Meta and Sama’s own  
20 business purposes for profit.

21           279. Plaintiffs and Class Members seek restitution and disgorgement of these unjust  
22 profits and revenues. Legal damages are inadequate to capture the full extent of Defendants’  
23 wrongdoing, their unjust benefits, and the harm their conduct caused to Plaintiffs and Class  
24 Members. For example, Plaintiffs’ and Class Members’ data can likely never be recovered from  
25 Meta’s systems, nor can Meta return the unjust benefits it gained by training its AI models using  
26 this data. Likewise, Plaintiffs cannot “reverse” the privacy harms caused by, for instance, Sama’s  
27 human review of their private videos. Legal damages are not sufficient to rectify this type of  
28

1 invasion, which is substantial. Restitution and disgorgement are thus appropriate to capture this  
2 wrongful conduct and irreparable harm.

3 280. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed  
4 under the statute and equity, including restitution; declaratory relief; reasonable attorneys' fees and  
5 costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate  
6 equitable relief permissible under the UCL.

7 **EIGHTH CLAIM FOR RELIEF**  
8 **Violations of the Consumers Legal Remedies Act (“CLRA”)**  
9 **Cal. Civ. Code §§ 1750 *et seq.***  
10 **(On Behalf of Plaintiffs and the Purchaser Subclass)**  
11 **(Against Meta & Luxottica)**

12 281. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with  
13 the same force and effect as if fully restated herein.

14 282. The CLRA prohibits unfair and deceptive practices in connection with the conduct  
15 of a business that provides goods, property, or services primarily for personal, family, or household  
16 purposes.

17 283. Meta and Luxottica are businesses that sell goods—Meta Smart Glasses—primarily  
18 for personal, family, or household purposes.

19 284. Meta and Luxottica engaged in unfair and deceptive practices in violation of the  
20 CLRA. Specifically, Meta and Luxottica violated the following provisions of the CLRA:

- 21 • Representing that goods have characteristics, uses, and benefits that they do  
22 not have. *See* Cal. Civ. Code § 1770(a)(5).
- 23 • Representing that goods are of a particular standard, quality, or grade when  
24 they were not. *See* Cal. Civ. Code § 1770(a)(7).
- 25 • Advertising goods or services with intent not to sell them as advertised. *See*  
26 Cal. Civ. Code § 1770(a)(9).
- 27 • Representing the subject of a transaction has been supplied in accordance  
28 with a previous representation when it has not. *See* Cal. Civ. Code §  
1770(a)(16).



1 property or to perform services” to disseminate any statement “which is untrue or misleading, and  
2 which is known, or which by the exercise of reasonable care should be known, to be untrue or  
3 misleading.” Cal. Bus. & Prof. Code § 17500.

4 292. It is also unlawful under the FAL to disseminate statements concerning property or  
5 services that are “untrue or misleading, and which is known, or which by the exercise of reasonable  
6 care should be known, to be untrue or misleading.” *Id.*

7 293. As alleged herein, the advertisements, practices, and representations released by  
8 Meta and Luxottica relating to Meta Smart Glasses were likely to mislead reasonable consumers as  
9 to how their private data would be collected, used, and disseminated, as well as the controls in place  
10 for consumers to limit or prohibit this conduct from occurring.

11 294. Meta and Luxottica’s business practices as alleged herein constitute unfair,  
12 deceptive, untrue, and misleading advertising pursuant to the FAL because Meta and Luxottica  
13 advertised the Meta Smart Glasses in a manner that is untrue and misleading. Defendants knew or  
14 reasonably should have known, that their false statements, coupled with omitted material  
15 information, would mislead Plaintiffs and the Class.

16 295. Meta and Luxottica profited from the sale of the falsely and deceptively advertised  
17 Meta Smart Glasses.

18 296. Plaintiffs and the Class are entitled to equitable relief, restitution, and disgorgement  
19 of the benefits conveyed on Meta and Luxottica. Plaintiffs and the Class also seek an order enjoining  
20 Meta and Luxottica from continuing to engage in deceptive business practices, false advertising,  
21 and any other act prohibited by law, including those set forth in this Complaint.

22 **TENTH CLAIM FOR RELIEF**  
23 **Breach of Express Contract**  
24 **(On Behalf of Plaintiffs and the Purchaser Subclass)**  
25 **(Against Meta & Luxottica)**

26 297. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with  
27 the same force and effect as if fully restated herein.

1           298. Meta and Luxottica entered into agreements with Plaintiffs and the other Purchaser  
2 Subclass Members in offering Meta Smart Glasses for sale, which Plaintiffs and the Purchaser  
3 Subclass Members purchased.

4           299. Meta and Luxottica’s privacy representations formed part of the contract between  
5 Meta and Luxottica, on the one hand, and Plaintiffs and the Purchaser Subclass Members on the  
6 other.

7           300. This includes:

- 8           1. Promising the Meta Smart Glasses come with “[p]rivacy . . . built-in” and  
9           that they had in place “important privacy safeguards”;
- 10           2. Promising that Meta would hold itself “accountable for protecting  
11           people’s privacy by regulators, policymakers, and experts” and that it  
12           “work[ed] with them to ensure that [Meta] . . . follows best practices and  
13           meets high standards for data protection”;
- 14           3. Promising that it would ensure “that people understand the types of data  
15           [Meta] use[s] to train the models that power our generative AI products”;
- 16           4. Promising that Meta Smart Glasses are “Designed for privacy, controlled  
17           by you.”
- 18           5. Promising that Meta AI is powered only by (1) “public content” like  
19           “profile info, comments, and posts”; (2) “interactions with AI features”  
20           like “questions you ask and images you ask Meta AI to imagine for you”;  
21           (3) other “public sources on the internet”; (4) “[i]nformation from  
22           partners”; and (5) “[l]icensed information.”

23           301. In light of these promises, which were used to sell and market Meta Smart Glasses,  
24 and formed a part of the bargain, Meta and Luxottica owed a contractual duty to Plaintiffs and the  
25 other Purchaser Subclass Members to honor their pledges and privacy assurances.

26           302. Meta and Luxottica breached this agreement because (1) Meta Smart Glasses were  
27 privacy invasive; (2) Meta Smart Glasses were not consistent with privacy expectations, best  
28

1 practices, or high standards for data protection; (3) there were no controls or opt-out mechanisms to  
2 prevent the collection, disclosure, or use of Plaintiffs' and the Purchaser Subclass Members' private  
3 audio, video, and other data; and (4) Meta AI was trained on Plaintiffs' and the Purchaser Subclass  
4 Members private audio, video, and other data, despite the claim that only a limited subset of data  
5 would be used for this purpose.

6 303. As a direct and proximate result of Meta and Luxottica's breach of contract, Plaintiffs  
7 and Purchaser Subclass Members sustained actual losses and damage as alleged herein, including  
8 that they did not receive the benefits of the bargains for which they paid and suffered privacy harms.  
9 As a further result of these breach(es), Meta was able to obtain the personal property of Plaintiffs  
10 and Purchaser Subclass Members in the form of their valuable private data.

11 304. Plaintiffs and the Purchaser Subclass Members seek compensatory damages,  
12 consequential damages in an amount to be proven at trial, and declarative, injunctive, or other  
13 equitable relief that may be appropriate. Plaintiffs and Purchaser Subclass Members alternatively  
14 seek an award of nominal damages.

15 **ELEVENTH CLAIM FOR RELIEF**  
16 **Breach of Implied Contract**  
17 **(On Behalf of Plaintiffs and the Nationwide Class)**  
18 **(Against Meta & Luxottica)**  
19 ***Pled in the Alternative as to the Purchaser Subclass***

20 305. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with  
21 the same force and effect as if fully restated herein.

22 306. When Plaintiffs and Purchaser Subclass Members used or were captured by Meta  
23 Smart Glasses, they entered into implied contracts with Meta and Luxottica, in which Meta and  
24 Luxottica agreed not to misappropriate, collect, use, or disclose their private data.

25 307. Meta and Luxottica solicited and invited Plaintiffs and Purchaser Subclass Members  
26 to use Meta Smart Glasses as part of their business practices. This included capturing video and  
27 audio content, as well as being personally captured by video and audio content taken on Meta Smart  
28 Glasses.

1 308. Plaintiffs and Purchaser Subclass Members agreed to use and/or be captured by  
2 Meta Smart Glasses with the reasonable belief that Meta and Luxottica’s privacy practices complied  
3 with relevant laws, regulations, and industry standards when they entered into the implied contracts  
4 with Defendants.

5 309. Plaintiffs and Purchaser Subclass Members would not have used Meta Smart  
6 Glasses, or allowed themselves to be captured in video and audio content taken on Meta Smart  
7 Glasses, had they known that Meta and Luxottica would not adhere to these implied promises.

8 310. Meta and Luxottica breached these implied contracts because (1) Meta Smart Glasses  
9 were privacy invasive; (2) Meta Smart Glasses were not consistent with privacy expectations, best  
10 practices, the laws described herein, or high standards for data protection; (3) there were no controls  
11 or opt-out mechanisms to prevent the collection, disclosure, or use of Plaintiffs’ and the Purchaser  
12 Subclass Members’ private audio, video, and other data; and (4) Meta AI was trained on Plaintiffs’  
13 and the Purchaser Subclass Members’ private audio, video, and other data.

14 311. As a direct and proximate result of Meta and Luxottica’s breach of these implied  
15 contracts, Plaintiffs and Purchaser Subclass Members sustained actual losses and damage as alleged  
16 herein, including that they did not receive the benefits of their bargains and suffered privacy harms.  
17 As a further result of these breach(es), Meta was able to obtain the personal property of Plaintiffs  
18 and Purchaser Subclass Members in the form of their valuable private data.

19 312. Plaintiffs and the Purchaser Subclass seek compensatory damages, consequential  
20 damages in an amount to be proven at trial, and declarative, injunctive, or other equitable relief that  
21 may be appropriate. Plaintiffs and Purchaser Subclass Members alternatively seek an award of  
22 nominal damages.

23 **TWELFTH CLAIM FOR RELIEF**  
24 **Negligence**  
25 **(On Behalf of Plaintiffs and the Nationwide Class)**  
26 **(Against Sama & Luxottica)**  
27 ***Pled in the Alternative***

28 313. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with  
the same force and effect as if fully restated herein.

1 314. While Sama and Luxottica’s conduct was by all means intentional, it was at the very  
2 least (and in the alternative) negligent.

3 315. Sama and Luxottica owed a duty to Plaintiffs’ and the Class to protect Plaintiffs’ and  
4 the Class’s private data. This duty arises from the highly sensitive nature of Plaintiffs’ and the  
5 Class’s data; the high likelihood of privacy harms that would be caused by the unauthorized  
6 collection, use, and disclosure of this information; the multiple statutes, regulations, and guidelines  
7 as described herein; and the common law.

8 316. Luxottica’s duty of care also arose as a result of, among other things, the special  
9 relationship that existed between Luxottica and Meta Smart Glasses purchasers. Luxottica was  
10 uniquely positioned to ensure that it was sufficiently protecting Plaintiffs’ and Class Members’  
11 sensitive personal information from unauthorized collection, use, or disclosure to third parties.

12 317. Sama and Luxottica breached their duties to exercise reasonable care in protecting  
13 Plaintiffs’ and Class Members’ sensitive personal information by agreeing, conspiring, effectuating,  
14 and/or receiving and using Plaintiffs’ and Class Members’ private communications, including audio  
15 and video captured on Meta Smart Glasses.

16 318. It was foreseeable to Sama and Luxottica that the unauthorized collection, disclosure,  
17 and use of Plaintiffs’ and Class Members’ sensitive personal information, including private audio  
18 and video, could result in injury to Plaintiffs and the Class.

19 319. As a direct and proximate result of Sama and Luxottica’s negligence, Plaintiffs and  
20 Class Members have been injured as described herein, and are entitled to damages, including  
21 compensatory, punitive, and nominal damages, in an amount to be proven at trial.

22 **THIRTEENTH CLAIM FOR RELIEF**  
23 **Unjust Enrichment**  
24 **(On Behalf of Plaintiffs and the Nationwide Class)**  
25 **(Against Meta)**  
26 ***Pled in the Alternative***

27 320. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with  
28 the same force and effect as if fully restated herein.

1 321. Meta received benefits from Plaintiffs and Class Members and unjustly retained  
2 those benefits at their expense.

3 322. Meta received benefits from Plaintiffs and Class Members in the form of the  
4 Plaintiffs' and Class Members' highly valuable data, including private audio and video, that Meta  
5 wrongfully intercepted, disclosed, and used, including to train its own AI models, without  
6 authorization and proper compensation.

7 323. Meta collected, disclosed, intercepted, stored, and used this data for its own gain,  
8 providing Meta with economic, intangible, and other benefits, including the ability to train its AI  
9 and ML models and algorithms.

10 324. Had Plaintiffs known of Meta's misconduct, they would not have used Meta Smart  
11 Glasses, demanded compensation, or paid significantly less for these products accompanied with  
12 privacy-invasive software.

13 325. Meta unjustly retained these benefits at the expense of Plaintiffs and Class Members  
14 because Meta's conduct caused irreparable privacy harms, caused Plaintiffs and Class Members to  
15 lose control of their private and valuable information, and placed them at an ongoing risk of future  
16 harm, all without providing any commensurate compensation to Plaintiffs and Class Members.

17 326. The benefits that Meta derived from Plaintiffs and Class Members rightly belong to  
18 Plaintiffs and Class Members. It would be inequitable under unjust enrichment principles in  
19 California for Meta to be permitted to retain any of the profit or other benefits they derived from the  
20 unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

21 327. Accordingly, Meta should be compelled to disgorge in a common fund for the benefit  
22 of Plaintiffs and Class Members all unlawful or inequitable proceeds that Meta received, and such  
23 other relief as the Court may deem just and proper.

24 **PRAYER FOR RELIEF**

25 WHEREFORE, Plaintiffs on behalf of themselves and the proposed Classes respectfully  
26 request that the Court enter an order:

- 1 A. Certifying the Classes and appointing Plaintiffs as the Classes’ representatives;
- 2 B. Finding that Defendants’ conduct was unlawful, as alleged herein;
- 3 C. Awarding declaratory relief against Defendants;
- 4 D. Awarding such injunctive and other equitable relief as the Court deems just and  
5 proper;
- 6 E. Awarding Plaintiffs and the Class Members statutory, actual, compensatory,  
7 consequential, punitive, and nominal damages, as well as restitution and/or  
8 disgorgement of profits unlawfully obtained;
- 9 F. Awarding Plaintiffs and the Class Members pre-judgment and post-judgment  
10 interest;
- 11 G. Awarding Plaintiffs and the Class Members reasonable attorneys’ fees, costs, and  
12 expenses; and
- 13 H. Granting such other relief as the Court deems just and proper.

14  
15 Dated: March 13, 2026

/s/Amber L. Schubert  
Robert C. Schubert #62684  
Willem F. Jonckheer #178748  
Amber L. Schubert #278696  
**SCHUBERT JONCKHEER &  
KOLBE LLP**  
2001 Union Street, Suite 200  
San Francisco, CA 94123  
Tel: (415) 788-4220  
Fax: (415) 788-0161  
rschubert@sjk.law  
wjonckheer@sjk.law  
aschubert@sjk.law

18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
Christian Levis (*pro hac vice* forthcoming)  
Amanda Fiorilla (*pro hac vice* forthcoming)  
Rachel Kesten (*pro hac vice* forthcoming)  
Katherine Boyd (*pro hac vice* forthcoming)  
**LOWEY DANNENBERG, P.C.**  
44 South Broadway, Suite 1100  
White Plains, NY 10601

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

Telephone: (914) 997-0500  
Facsimile: (914) 997-0035  
clevis@lowey.com  
afiorilla@lowey.com  
rkesten@lowey.com  
kboyd@lowey.com