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

FRANCISCO ALVAREZ; F.M.A., a minor, by and through his guardian Francisco Alvarez; JEREMY WAHL; I.W., a minor, by and through her guardian Jeremy Wahl, individually and on behalf of all others similarly situated, Plaintiffs, *v.* META PLATFORMS, INC., Defendant.	Case No.

CLASS ACTION COMPLAINT

Table of Contents

Page

I. Introduction 1

II. Parties 13

A. Plaintiffs 13

B. Defendant 15

III. Jurisdiction and Venue 16

IV. Factual Allegations 17

A. Meta Glasses and NameTag: the "dystopian privacy invasion" nobody asked for. 17

B. Generative AI: A new front in Meta's war on privacy 27

1. Meta pivots from the "metaverse" to AI. 27

2. Meta's text-to-image generative AI models and products 30

3. Meta's use of Facebook and Instagram images to train and test its text-to-image GenAI models results in the creation and storage of biometric identifiers and information within the models themselves. 33

4. When a user submits an image of a person's face to one of Meta's text-to-image GenAI models via prompting (the inference stage), the model likewise creates and stores a biometric identifier of biometric information associated with the person in the image. 40

C. Meta profited from its collection and use of Plaintiffs' and Class Members' images and biometric data, and Plaintiffs and Class Members were injured by Meta's wrongful conduct. 42

D. Delayed Discovery, Equitable Tolling, and Fraudulent Concealment 45

V. Class Action Allegations 47

VI. Claims for Relief 51

CLAIM 1: Violation of Section 15(a) of the Illinois Biometric Information Privacy Act (by Plaintiffs Francisco Alvarez and I.W., a minor proceeding by and through his guardian Francisco Alvarez, on Behalf of Themselves and Members of the Illinois Class) 51

CLAIM 2: Violation of Section 15(b) of the Illinois Biometric Information Privacy Act Information Privacy Act (by Plaintiffs Francisco Alvarez and

I.W., a minor proceeding by and through his guardian Francisco Alvarez, on Behalf of Themselves and Members of the Illinois Class) 53

CLAIM 3: Violation of California Common Law – Right of Publicity (by all Plaintiffs, on Behalf of Themselves and the National Class, and by Jeremy Wahl and I.W., a minor proceeding by and through her guardian Jeremy Wahl, on Behalf of Themselves and the California Class) 54

CLAIM 4: Violation of California Civil Code § 3344(a) – Commercial Misappropriation (by all Plaintiffs, on Behalf of Themselves and the National Class, and by Jeremy Wahl and I.W., a minor proceeding by and through her guardian Jeremy Wahl, on Behalf of Themselves and the California Class) 56

CLAIM 5: Violation of California Constitution – Right to Privacy (by Plaintiffs Jeremy Wahl and I.W., a minor proceeding by and through her guardian Jeremy Wahl, on Behalf of Themselves and the California Class) 58

VII. Prayer For Relief 61

VIII. Jury Demand 62

Plaintiffs Francisco Alvarez; F.M.A., a minor, by and through his guardian Francisco Alvarez; Jeremy Wahl; I.W., a minor, by and through her guardian Jeremy Wahl, individually and on behalf of all others similarly situated, bring this action against Defendant Meta Platforms, Inc., individually and on behalf of all others similarly situated, and allege the following based on personal knowledge, the investigation of counsel, and information and belief.

I. INTRODUCTION

1. This case is about Meta's latest attempts to turn the personal information of billions of people into profit. Over the past few years, the company has harvested and exploited the biometric data of its platforms' users and other members of the public to build facial-recognition and generative-AI technologies without providing the notice or obtaining the consent required by law. These latest privacy violations by Meta are not an aberration, but the foreseeable consequence of a business model that has for over 20 years depended on collecting, analyzing, and monetizing ever-greater amounts of personal data.

2. In 2003 Mark Zuckerberg—at the time a 19-year-old Harvard student—launched a website called Facemash. The site displayed pairs of Harvard students' photos and asked users to choose who was more attractive, similar to the then-popular "Hot or Not" website.

3. Zuckerberg had obtained the images by scraping students' ID photos from Harvard's online directories without permission. The students had not consented to having their photos copied and repurposed for Zuckerberg's version of Hot or Not.

4. Facemash was available for only a few days before Zuckerberg took it down, likely because he was accused by Harvard's Administrative Board of "violating individual privacy, breaching security, and violating copyrights."[1]

5. After taking the site down, "Zuckerberg decided that criticism of the site was too strong to re-post it. 'Issues about violating people's privacy don't seem to be surmountable,' he wrote at that point. 'I'm not willing to risk insulting anyone.'"[2]

6. Notwithstanding his purported concerns about privacy, four months later Zuckerberg launched Facebook, the social-media site that is now operated by Defendant Meta Platforms, Inc., of which Zuckerberg is the CEO.

7. Shortly after launching Facebook, which was originally accessible only to Harvard students, Zuckerberg messaged a friend offering information—including emails, pictures, addresses, and SNS [Social Security numbers]"—about "anyone at Harvard" and referring to those who had trusted him with their personal information as "dumb f****":[3]

[1] Anaya Nolan, *Zuckerberg's Facemash: Legal Or Lawless?*, LAW SHUN (Mar. 19, 2025), https://lawshun.com/article/what-laws-did-zuckerberg-break-facemash.

[2] Katharine A. Kaplan, *Facemash Creator Survives Ad Board*, THE HARVARD CRIMSON (Nov. 19, 2023), https://www.thecrimson.com/article/2003/11/19/facemash-creator-survives-ad-board-the/.

[3] Pranav Dixit, *Mark Zuckerberg's old chat calling Facebook users 'dumb' resurfaces, see Elon Musk's reaction*, BUSINESS TODAY (July 8, 2023), https://www.businesstoday.in/technology/news/story/mark-zuckerbergs-old-chat-calling-facebook-users-dumb-resurfaces-see-elon-musks-reaction-388849-2023-07-08.

8. Today Meta is one of the largest, most successful, and most powerful companies in the world. Founded in 2004, Meta owns Facebook, Instagram, WhatsApp, and Messenger—platforms that collectively reach billions of users globally and play a leading role in how people communicate, share information, consume content, and interact online.

9. In fiscal year 2024, Meta generated approximately $200.97 billion in revenue and $60.46 billion in net income. As of mid-2026, its market value exceeded $1.6 trillion and the company was ranked number 17 on the 2025 Fortune 500 list, which tabulates the largest U.S. companies by revenue, and number 41 on the 2025 Fortune Global 500, placing it among the world's most economically significant corporations. Through its control of some of the world's most widely used social-media and messaging services, and its massive investments in artificial intelligence (AI), virtual reality, and digital advertising, Meta exerts extraordinary influence over global communications, commerce, technology development, and the flow of information.

10. Meta's remarkable financial success is closely tied to its ability to collect, analyze, and monetize vast amounts of user data across Facebook, Instagram, WhatsApp,

Messenger, and other services. The company generates the overwhelming majority of its revenue through digital advertising, which depends on detailed information about users' demographics, interests, online behavior, social connections, location, engagement patterns, and interactions with content and advertisers. This data enables Meta to offer highly targeted advertising that is generally more valuable to advertisers than untargeted advertising, helping drive the company's astronomical profits.

11. Through access to data generated by billions of users worldwide, Meta has been able to build and refine some of the world's most sophisticated advertising, recommendation, and AI systems. The scale of that data ecosystem is a significant competitive advantage that has helped Meta become one of the world's most valuable corporations, with a leading position in both digital advertising and artificial intelligence.

12. But Zuckerberg's disregard for the privacy rights of his platforms' users and the public in general seems to have changed little since his Facemash days.

13. Over the past seven years alone, Meta has paid more than $10 billion in government fines and class-action settlements for violations of its users' privacy rights, including $5 billion in civil penalties to the FTC, approximately $1.3 billion in fines for violations of the General Data Protection Regulation in the European Union, a $725 million settlement for improperly sharing user data with third parties such as Cambridge Analytica, a $650 settlement stemming from violations of the Illinois Biometric Information Privacy Act (BIPA), and a $1.4 billion settlement in connection with violations of the Texas Capture or Use of Biometric Identity Act.

14. But even these hefty penalties seem to have done little to deter the $1.3 *trillion* company from playing fast and loose with its users' data.

15. Since at least 2024, Meta has publicly acknowledged that it uses information from user-generated content and interactions on its platforms to develop and improve artificial-intelligence technologies, including its generative AI models and AI systems.[4]

16. Unfortunately, Meta has not been transparent with users about *which* of their data it is using and *how* it is doing so.

17. Recent reporting and research have revealed that Meta collects and stores the biometric data of users and non-users of its products alike, and both Meta's selective statements and its secrecy reflect that it is doing so without disclosure or consent, in violation of the laws of Illinois and California, the state where it is headquartered.

18. Specifically, Meta has been collecting images of people's faces uploaded to Facebook or Instagram and using those images to train the AI model that powers a facial-recognition feature called NameTag for Meta's Ray-Ban and Oakley smart glasses (Meta Glasses) and the Meta AI companion app, and also to generate biometric identifiers for use by NameTag.

19. For years, Meta has indicated that it was considering building facial-recognition capabilities into its smart glasses. In June 2026, it was discovered that Meta had indeed built such a facial-recognition system and was ready to deploy it for use by Meta Glasses, its latest line of smart glasses.

[4] An AI *model* is a trained computational system, consisting of an architecture and learned parameters, that generates outputs from inputs. An AI *system* is broader: it includes the model together with additional software components that process inputs, present outputs, and interact with users. *See generally* Yuanyuan Sun, et al., *Defining AI Models and AI Systems: A Framework to Resolve the Boundary Problem*, ARXIV (Mar. 12, 2026), *available at* https://arxiv.org/html/2603.10023v1.

20. That month, journalists reported that they had uncovered "an unreleased face-recognition system embedded in Meta's smart glasses platform"—the Meta AI app on a user's smartphone that pairs with Meta Glasses.[5] This discovery showed "that Meta had begun shipping face-recognition code to users' phones while publicly describing it as something the company was still 'thinking through.'"[6]

21. Though it was not yet enabled, NameTag sat "inside a Meta AI companion app that[ ] [had] been downloaded over 50 million times and is necessary for use of key features of its smart glasses … ."[7]

22. Once activated, NameTag would "transform faces captured by Meta's glasses into unique biometric signatures, commonly known as faceprints, and check each one against faceprints stored on the user's phone—**a database that's currently configured to receive updates from Meta**."[8]

23. How would NameTag be able to link a captured image of a face to a name? We know the answer thanks to two Meta employees, who stated earlier in 2026 that "[p]ossible options include recognizing people a user knows because they are connected on

[5] Dhruv Mehrorta & Dell Cameron, *Meta Silently Added Face-Recognition Code for Its Smart Glasses to Millions of Phones*, WIRED (June 4, 2026), https://www.wired.com/story/meta-smart-glasses-face-recognition-nametag-connections/.

[6] *Id.*

[7] *Id.*

[8] *Id.* (emphasis added).

a Meta platform, and identifying people whom the user may not know but who have a public account on a Meta site like Instagram."[9]

24. In other words, NameTag would work by collecting images of faces from user-generated content on Meta's platforms (including Facebook and Instagram), using those images to create biometric identifiers and information associated with those users, storing the biometric identifiers on Meta's servers, and then providing them to NameTag so that they could be used by NameTag to identify people recorded by the company's Meta Glasses.

25. The biometric identifiers and information generated by NameTag and collected and stored by Meta are numerical representations corresponding to faces detected in images uploaded by users of Meta platforms.

26. These numerical representations—sometimes called, among other things, face embeddings, face vectors, face encodings, facial representations, or face prints—are created by the facial-recognition model extracting information associated with the facial features, such as edges of different orientations; contours; and shapes of the eyes, nose, and lips, as well as the spatial relationships between those facial features.

27. Meta did all of this without providing notice to—or obtaining consent from—the users of its platforms or the non-users appearing in the images from which Meta extracted biometric identifiers and information.

[9] Kashmir Hill, et al., *Meta Plans to Add Facial Recognition Technology to Its Smart Glasses*, THE NEW YORK TIMES (updated Feb. 14, 2026), https://www.nytimes.com/2026/02/13/technology/meta-facial-recognition-smart-glasses.html.

28. Meta hid the existence of NameTag because it understood that its users and the public at large would be outraged by Meta's conduct. As shown by an internal memo obtained by the New York Times, Meta planned to divert public attention away from its launch of this dystopian surveillance technology by timing the release of the NameTag feature to take advantage of "political tumult in the United States":

> Meta's internal memo said the political tumult in the United States was good timing for the feature's release.
>
> "We will launch during a dynamic political environment where many civil society groups that we would expect to attack us would have their resources focused on other concerns," according to the document from Meta's Reality Labs, which works on hardware including smart glasses.[10]

29. Facial-recognition models such as those that power NameTag are sometimes referred to as "perceptive AI," a category of AI that is trained to recognize, for example, faces, objects, speech, or events in data such as images or audio.

30. In addition to appropriating user-uploaded images to train and implement the NameTag facial-recognition features (perceptive AI), Meta has also collected and used those images to train and implement its *generative* AI (or GenAI) models, including Emu, CM3leon, Chameleon, and Muse Image.

31. This is significant because, although the primary purpose of AI models is to create new content such as text, images, audio, video, or computer code in response to a user's prompt, these models have often been found to have strong *perceptive* abilities as well—abilities such as recognizing faces, identifying objects in images, and answering questions about an image.

[10] *Id.*

32. That is because, just like perceptive AI models, GenAI models that are trained on images of people's faces (1) extract information associated with the facial features, such as edges of different orientations; contours; and shapes of the eyes, nose, and lips, as well as the spatial relationships between those facial features; (2) convert that information into a numerical representation; and (3) associate that numerical representation with personally identifiable information, such as a name.

33. Moreover, this training process results in these numerical representations and their associated personally identifiable information (which collectively constitute a biometric identifier or biometric information) being forever stored in the code of the GenAI model that the image was used to train.

34. A similar process occurs during the inference phase—namely, when a fully trained GenAI model uses its learned patterns to process new, previously unseen inputs and to generate novel outputs.

35. For example, when a user uploads an image of a face to one of Meta's GenAI models, the image is converted into a numerical representation (sometimes called an embedding, a latent representation, or a feature vector) and stored for an undisclosed length of time by Meta.

36. Meta has long boasted about having an edge over its competitors in the AI space because, unlike them, Meta has access to countless quality images uploaded to Facebook and Instagram that it used to train its AI models:

> We know OpenAI, Google, Microsoft, the folks playing here, a lot of the energy goes into the less easily measurable, but very toilsome and important work of data quality.

> **Our data advantage is really the public images that have been shared on Facebook and Instagram**, as well as the public text. So we don't train on private stuff, we don't train on stuff that people shared with their friends; we do train on things that are public.
>
> And if you look at our image model—Emu is its name—if you use Imagine in one of our products, you'll use our text-to-image model. **You get really amazing quality images and a lot of that is because Instagram is the data set that was used to train it**, which is just one of the great repositories of incredible imagery. A lot of different types of art, fashion, you know, culture, and **also just imagery of people and us**.[11]

37. While AI engineers and investors are familiar with Meta's exploitation of its users' data, consumers and the public more broadly are largely ignorant of Meta's collection, storage, and use of their data, including biometrics. This is by design.

38. While Meta states in one of its policies that it trains its AI models using "[i]nformation shared on Meta Products including things like posts or photos and their captions, and [users'] interactions with features that are part of AI at Meta,"[12] this statement is vague and difficult to find, as it appears neither in Meta's 5,386-word Terms of Service[13] nor its 21,118-word Privacy Policy,[14] but rather in a separate document tucked away in a corner of Facebook's website that few users visit or are even aware of.

---

[11] *Meta's Cox on Building AI Into the Product Suite*, at 6:09–7:01 (BLOOMBERG, May 9, 2024) (emphasis added), https://www.bloomberg.com/news/videos/2024-05-09/meta-s-cox-on-building-ai-into-the-product-suite-video.

[12] *How Meta uses information for generative AI models and features*, META (July 30, 2026), https://www.facebook.com/privacy/genai?entry_point=POLICY_SUBPAGE%3Abanner.subpage.agentic-ai-2026-h1-eu.

[13] *Terms of Service*, META (July 30, 2026), https://mbasic.facebook.com/legal/terms/plain_text_terms/.

[14] *Privacy Policy*, META (July 30, 2026), https://www.facebook.com/privacy/policy/.

39. The fact that Facebook and Instagram users have not consented to—and do not *want*—Meta's AI models to use their images was vividly illustrated by the backlash to Meta's July 2026 launch of Muse Image, "the first image generation model from Meta Superintelligence Labs."[15]

40. Among other things, Muse Image added a feature to "Instagram that allowed users to generate images based on people's public accounts": "The feature … automatically opted in any Instagram user with a public account. As a result, countless people's likenesses were used in A.I. images without their consent. Users complained about privacy and copyright concerns."[16]

41. Facing immediate and widespread criticism, Meta withdrew the feature from Instagram three days after launch, stating: "We've heard the feedback that this feature missed the mark, so it's no longer available."[17]

42. Contrary to its public statements, Meta **did not** get rid of the controversial feature. While the company removed the Muse Image feature from the *Instagram app*, anyone can still access the same feature by going to the Meta AI homepage (meta.ai) or downloading the Meta AI app, and from there prompting Meta AI to create a deepfake from a public Instagram account holder's image.

---

[15] *Introducing Muse Image: Image Generation Built for Your World*, META (July 7, 2026), https://about.fb.com/news/2026/07/introducing-muse-image-meta-ai/.

[16] *Meta Removes A.I. Feature on Instagram After Days of Backlash*, META (July 10, 2026), https://www.nytimes.com/2026/07/10/technology/meta-muse-images-instagram-removal.html.

[17] *Id.*

43. In other words, the feature that propelled Instagram users to complain en masse about privacy and copyright violations is still active and accessible without restrictions.

44. Meta's covert preparations to deploy NameTag and its rollout of Muse Image generally follow the same pattern as Meta's myriad other privacy violations over the last two decades: Meta launches a feature that expands data collection or diminishes privacy by default, faces public or regulatory backlash, and then either withdraws the feature or apologizes while preserving the feature's core function.[18]

45. Thus, while Meta has removed the NameTag source code from the Meta AI app and made the controversial Muse Image feature unavailable *directly* through the Instagram app, it has **not** disclosed, apologized for, or ceased its collection, storage, and use of people's images and biometrics to train and implement the AI models underlying either NameTag's facial-recognition features or Meta's GenAI platforms.

46. In sum, Meta obtained images of Plaintiffs and Class Members through Meta platforms such as Facebook and Instagram, and then wrongfully collected, stored, used, and profited from those images and the biometric identifiers and information extracted from them, thereby harming the substantive privacy interests of Plaintiffs and Class Members, and violating the laws of the States of Illinois and California, including the Illinois

[18] *See generally* SHEERA FRENKEL & CECILIA KANG, AN UGLY TRUTH: INSIDE FACEBOOK'S BATTLE FOR DOMINATION (2021) (recounting Facebook's 20-year pattern of privacy violations and concluding that "the social network's massive gains have repeatedly come at the expense of consumer privacy and safety and the integrity of democratic systems").

Biometric Information Privacy Act § 15(a)–(c), the right of publicity under California common law, California Civil Code § 3344(a), and the California Constitution.

II. PARTIES

A. Plaintiffs

47. Plaintiff Francisco Alvarez is a natural person and citizen of the State of Illinois.

48. Plaintiff F.M.A., a minor, and his parent and guardian Francisco Alvarez, are natural persons and citizens of the State of Illinois.

49. Mr. Alvarez has two Facebook accounts and one Instagram account.

50. He has had a Facebook account for approximately 15 years and an Instagram account for approximately 10 years.

51. All of the accounts are for personal use.

52. Mr. Alvarez posted new content—such as photos of himself, his friends, and his family—to his Facebook and Instagram accounts every three to four months on average.

53. F.M.A.'s mother also has an Instagram account and posted a selfie of herself and F.M.A., as her profile picture when F.M.A. was around three years old.

54. At the time, the Facebook and Instagram accounts of both Mr. Alvarez and F.M.A.'s mother were public.

55. Plaintiff Jeremy Wahl is a natural person and citizen of the State of California.

56. Plaintiff I.W., a minor, and her parent and guardian Jeremy Wahl, are natural persons and citizens of the State of California.

57. Mr. Wahl has two Facebook accounts (one for personal use and one for business use) and one Instagram account.

58. Mr. Wahl has had a Facebook account for approximately 20 years, and an Instagram account for approximately 10 years.

59. Mr. Wahl has posted photos of himself and his minor daughter, I.W., to the accounts, including photos of I.W. throughout her life, from when she was a baby, a toddler, celebrating her birthday, and attending a friend's birthday party.

60. As of the time of the filing of this Complaint, I.W. is 10 years old.

61. Mr. Wahl's Facebook account was completely public until about two years ago, when he restricted access to some of the information he posted.

62. Mr. Wahl's Instagram account has always been public.

63. Upon information and belief, images of each of Plaintiff's faces has been used by Meta in one or more of the following ways: (1) to train the facial-recognition model used by NameTag; (2) to create a face embedding, face vector, face template, or equivalent information using the facial-recognition model employed by NameTag; (3) to train Meta's generative AI models, including but not limited to Emu and Muse Image; or (4) to create an output from one of Meta's generative AI models, including but not limited to Emu and Muse Image, through a user submitting the image via prompt as an input to one of Meta's generative AI models during the inference stage.

64. Although Meta never notified Plaintiffs that their images and biometric data were being collected and used for these specific purposes, information that first became public in mid-2026 strongly suggests that this is the case.

65. Specifically, within the span of a month, news broke that the code for the NameTag facial-recognition feature had been installed on the Meta AI app for use with Meta Glasses *and* that the Muse Image feature had been integrated with Instagram to allow users to generate images in Meta AI by @-mentioning public Instagram accounts—with both stories resulting in public outcry.

66. Further investigation revealed that Meta had used images from Facebook and Instagram in the ways alleged in this Complaint, thereby generating, storing, and using the biometric identifiers and information of people appearing in those images.

67. Meta has never disclosed *which* Facebook and Instagram images it has collected biometric data from; this information is solely within Meta's possession, custody, or control.

68. Nonetheless, Meta has publicly boasted of using images from Facebook and Instagram to train its various AI models, and its earliest consumer-facing image-generation model, Emu, was trained using 1.1 billion images.

69. Given that Meta has trained numerous image-generation models in addition to Emu, including the recently released Muse Image, Meta has used *at least* several billion Facebook and Instagram images to train its image-generation models.

B. Defendant

70. Defendant Meta Platforms, Inc., is a Delaware corporation with a principal place of business at 1 Meta Way, Menlo Park, California 94025.

71. Among other services, Meta has developed, owns and operates several major social-media and messaging platforms including: Facebook since its launch in 2004; Messenger since its launch as Facebook Chat in 2008; Instagram since its acquisition in

2012; and WhatsApp since its acquisition in 2014. These platforms are amongs the most used social platforms in the world, with Facebook reporting 3.07 billion monthly users (number one overall), Instagram reporting 2.8 billion monthly users (number two overall), WhatsApp reporting 2 billion monthly users (number four overall), and Messenger reporting 1.01 billion monthly users (number six overall).

III. JURISDICTION AND VENUE

72. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) ("CAFA"), because: (i) the proposed Class consists of well over 100 persons; (ii) the parties are minimally diverse, as members of the proposed Class—including Plaintiffs Francisco Alvarez and F.M.A., a minor proceeding by and through his guardian Francisco Alvarez—are citizens of a state different from Defendant's home state; and (iii) the aggregate amount in controversy exceeds $5 million, exclusive of interests and costs.

73. This Court has personal jurisdiction over Plaintiffs because Plaintiffs submit to the Court's jurisdiction. This Court has personal jurisdiction over Defendant Meta because Meta deliberately targeted and exploited the Illinois market by acquiring millions of Facebook and Instagram users in the state. Meta has collected, stored, used, and profited from the images of those users and the biometric data harvested from those images. Meta also has collected, stored, used, and profited from the images of non-user Illinois residents uploaded to Meta's platforms and the biometric data harvested from those images. Plaintiffs' claims therefore arise out of or relate to Meta's contacts with the state of Illinois.

74. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the acts or omissions giving rise to the claims occurred in this District.

Alternatively, venue is proper under 28 U.S.C. § 1391(b)(3) because this Court has personal jurisdiction over Defendant Meta.

IV. FACTUAL ALLEGATIONS

A. Meta Glasses and NameTag: the "dystopian privacy invasion" nobody asked for.

75. In September 2020 Meta CEO Mark Zuckerberg first announced that Meta and EssilorLuxottica would be collaborating "to develop the next generation of smart glasses."[19] Over the next 6 years, Meta released three different lines of smart glasses: (1) Ray-Ban Stories in September 2021; (2) Ray-Ban Meta in September 2023; and (3) Meta Glasses in June 2026.

76. Notably, Meta has been considering incorporating facial-recognition technology into its smart glasses since before the 2021 release of Ray-Ban Stories.[20]

77. The company was aware from the beginning that the public may not want such an invasive feature embedded in eyewear, as evidenced by the February 2021 statements of Meta executive Andrew Bosworth:

> "It's really a debate we need to have with the public," Bosworth added. "If people don't want this technology, we don't have to supply it. The product is going to be fine either way. There are some nice use cases out there, if it's something people are comfortable with."

---

[19] *Facebook and EssilorLuxottica Announce Collaboration for Smart Glasses*, ESSILORLUXOTTICA (Sept. 16, 2020), https://www.essilorluxottica.com/en/newsroom/press-releases/facebook-essilorluxottica-collab/.

[20] *See, e.g.*, Salvador Rodriguez, *Facebook is 'looking at' facial recognition technology for upcoming smart glasses, executive confirms*, CNBC (Feb. 25, 2021) ("Asked if 'Facebook is considering offering facial recognition on its smart glasses products?,' [Meta Executive Andrew] Bosworth said, 'We're looking at it.'"), https://www.cnbc.com/2021/02/25/facebook-looking-at-facial-recognition-technology-andrew-bosworth.html.

> …
>
> Bosworth noted that there are ethical concerns with the numerous ways that face recognition and always-on cameras and microphones could be abused.
>
> "All the ways they can be abused, in particular for marginalized communities by authority structures," Bosworth said. "What are all the ways that we can prevent those? And is it enough?"[21]

78. The public debate that Bosworth indicated was a necessary precondition for adding a facial-recognition feature to Meta's smart glasses never happened.

79. While Meta "originally scrapped the facial recognition feature for the first generation of the Ray-Ban Meta AI glasses over ethical concerns," by 2025 "a more business friendly Federal Trade Commission under the new Trump Administration had emboldened Meta to reboot its plans for the next generation of smart glasses."[22]

80. As one reporter put it: "It's the latest example of AI-powered tech creeping into your private life, whether you like it or not."[23]

81. A few months before Meta's June 2026 release of Meta Glasses, its latest line of smart glasses, executive Andrew Bosworth confirmed "that the company [was] 'looking at' incorporating facial recognition technology for its upcoming smart glasses devices."[24] As reported by the New York Times, "[t]he feature, internally called 'Name Tag,' would let

---

[21] *Id.*

[22] *Cecily Mauran*, *Meta forges ahead with facial recognition for its AI glasses*, MASHABLE (May 8, 2025), https://mashable.com/article/meta-facial-recognition-ai-glasses-privacy-concerns.

[23] *Id.*

[24] *Id.*

wearers of smart glasses identify people and get information about them via Meta's artificial intelligence assistant."[25]

82. The reporting on Meta's plans to include facial-recognition features with its smart glasses led to a public outcry. In an April 2026 open letter co-signed by 75 local, state, and national organizations that advocate for domestic violence survivors, worker rights, bodily autonomy, consumer privacy, civil rights, and civil liberties, the ACLU "urge[d] Meta to immediately halt and publicly disavow its plans to deploy facial recognition features on its Ray-Ban and Oakley glasses, including the feature reportedly known internally as 'Name Tag.'"[26]

83. The letter described in detail how facial recognition paired with Meta Glasses would "represent[ ] a serious threat to privacy and civil liberties for every member of our society":

> Adding facial recognition and/or "Name Tag" technology would let anyone wearing a pair surveil and profile every person they encounter — without those people ever knowing. … It is inevitable that this technology will exacerbate abuse, harassment, and stalking of women, girls, and LGBTQ+ people, and will place children in danger. To outline just a couple of examples: perpetrators could use 'Name Tag' to identify and stalk victims, and abusers could use it to identify, track, and harm children. This invasion of privacy is also primed to be coopted for police surveillance, circumventing the Fourth Amendment, and

[25] Kashmir Hill, et al., *Meta Plans to Add Facial Recognition Technology to Its Smart Glasses*, THE NEW YORK TIMES (updated Feb. 14, 2026), https://www.nytimes.com/2026/02/13/technology/meta-facial-recognition-smart-glasses.html.

[26] Letter to Meta at 2 (Apr. 13, 2026), *available at* https://www.aclum.org/app/uploads/2026/04/Sign-On-Letter-to-Meta-Regarding-Facial-Recognition-Features-on-Meta-Glasses-April-14.pdf.

> disproportionately harming Black, Brown, immigrant, and other over-policed communities.
>
> But it's not just these vulnerable groups at risk.
>
> Corporate dissidents could use this technology to identify and harass leadership at pharmaceutical, insurance, oil, or other major companies as they go about their daily lives. Politicians and their staff would forfeit any ability to move through the country in relative anonymity. Abortion or IVF foes could stake out clinics and identify everyone coming and going. And when facial recognition technology is combined with the huge wealth of data that Meta and other tech companies hold on most Americans, the risks become even starker. Stalkers and scammers using the tech could conceivably find out, quickly and in complete stealth, not just the name of the person sitting next to them on the subway—but their address, marital status, social media profiles, workplace, income, hobbies, health information, and habits. That's frightening to contemplate.[27]

84. As the letter noted: "The American people have not consented to this dystopian privacy invasion, and indeed there is no way to obtain meaningful consent of all people impacted."[28]

85. Meta appears to agree that it is impossible to obtain informed consent from impacted individuals. So rather than making an effort to obtain such consent, the company has attempted to outsource that obligation and related consequences to Meta Glasses users, brazenly asserting in one of its "supplemental" terms of service that users, *not Meta*, are "responsible for … providing any notice to or obtaining any consents from other individuals

[27] *Id.*

[28] *Id.*

who [they] interact with on [their] [Meta] Products as may be required under video recording, audio recording, biometric data, or other privacy or data protection laws."[29]

86. The privacy concerns catalogued in the ACLU's letter are well-founded, as—even without a facial-recognition feature—Meta Glasses have been used to sexually harass women so often that they are commonly referred to as "pervert glasses":

> Men are using the camera glasses to film women who do not know it is happening, and not only on the street. It is happening in gyms, in bathrooms and in change rooms. The footage lands on Instagram and TikTok, where the women in it are identified and mocked in the comments.
>
> For these reasons, news outlets such as The Guardian, Wired and Vox, among countless others, have dubbed them "pervert glasses," a term that also found its way into a recent Jimmy Kimmel monologue and skit.[30]

87. Meta did not respond to the ACLU's letter, nor did it heed the letter's call to publicly disavow its plans to deploy its NameTag facial-recognition features on Meta Glasses.

88. Instead, Meta continued its preparations to launch Meta Glasses with the NameTag feature in the midst of political turmoil in the United States—when civil-society groups like the ACLU "would have their resources focused on other concerns."[31]

---

[29] *Supplemental Meta Platforms Technologies Terms of Service*, Meta, (last updated Apr. 29, 2025) https://www.meta.com/legal/supplemental-terms-of-service/?srsltid=AfmBOoo0GM3SiomuiCBo-F6w5maQKnc3vrwBHpbbegYhGNhxqIqqIfWt.

[30] Mason Kossak, *The internet is calling them 'pervert glasses.' Here's what Meta's smart glasses can actually do*, NATIONAL POST (Aug. 18, 2026), https://nationalpost.com/news/meta-glasses-recording-no-way-of-knowing.

[31] Kashmir Hill, et al., *Meta Plans to Add Facial Recognition Technology to Its Smart Glasses*, THE NEW YORK TIMES (updated Feb. 14, 2026), https://www.nytimes.com/2026/02/13/technology/meta-facial-recognition-smart-glasses.html.

89. Meta's plan to take advantage of political tumult is particularly disturbing given that several studies have found that social-media platforms like Facebook "intensif[y] divisiveness and thus contribut[e] to [the] corrosive consequences" of "U.S. political polarization."[32]

90. Shortly after Meta Glasses were released to the public in June 2026, journalists discovered that Meta had "quietly embedded face-recognition technology [NameTag] for its smart glasses" into the Meta AI app—which is installed on users' phones and pairs with Meta Glasses.[33]

91. "The discovery of NameTag in the live Meta AI app shows that Meta had begun shipping face-recognition code to users' phones while publicly describing it as something the company was still 'thinking through.'"[34]

92. The revelation that the NameTag facial-recognition technology was installed on users' phones and ready to launch with the turn of a key alerted the public to Meta's collection and storage of their biometric identifiers extracted through photos uploaded to Facebook and Instagram.

---

[32] Paul M. Barrett, et al., *Fueling the Fire: How Social Media Intensifies U.S. Political Polarization—And What Can Be Done About It* at 1, NYU STERN CENTER FOR BUSINESS AND HUMAN RIGHTS (Sept. 2021), *available at* https://bhr.stern.nyu.edu/wp-content/uploads/2024/02/NYUCBHRFuelingTheFire_FINALONLINEREVISEDSep7.pdf.

[33] Dhruv Mehrorta & Dell Cameron, *Meta Silently Added Face-Recognition Code for Its Smart Glasses to Millions of Phones*, WIRED (June 4, 2026), https://www.wired.com/story/meta-smart-glasses-face-recognition-nametag-connections/.

[34] *Id.*

93. Investigation of the code revealed that "as early as January [2026]"—five months before Meta Glasses were even available for purchase—core components of the [NameTag] system had been integrated into software distributed to millions of people."[35]

94. When activated, the NameTag feature would "transform faces captured by Meta's glasses into unique biometric signatures, commonly known as faceprints, and check each one against faceprints stored on the user's phone—a **database that's currently configured to receive updates from Meta**."[36]

95. In other words, Meta had a collection of biometric identifiers and information in the form of faceprints on its servers that it is ready to use for facial recognition via NameTag. Once the NameTag feature is activated by Meta, any image of a person's face captured by Meta Glasses would be analyzed to extract a faceprint that would then be matched against Meta's storehouse of faceprints for purposes of facial recognition.

96. This describes exactly the two possibilities that Meta employees disclosed to the New York Times four months before Meta Glasses were released: "Possible options include recognizing people a user knows because **they are connected on a Meta platform**, and identifying people whom the user may not know but **who have a public account on a Meta site like Instagram**."[37]

---

[35] *Id.*

[36] *Id.* (emphasis added).

[37] Kashmir Hill, et al., *Meta Plans to Add Facial Recognition Technology to Its Smart Glasses*, THE NEW YORK TIMES (updated Feb. 14, 2026) (emphasis added), https://www.nytimes.com/2026/02/13/technology/meta-facial-recognition-smart-glasses.html.

97. Both of these options involve Meta collecting and storing biometric identifiers of people who appear in an image on Facebook or Instagram.

98. Regardless of which of these two options Meta ultimately implemented when creating NameTag, publicly available information shows that NameTag works by comparing the biometric identifiers and information extracted from images captured by Meta Glasses and comparing them to the biometric data obtained from images obtained from Facebook and Instagram that are stored on Meta's servers.

99. This conclusion is further supported by a patent application published in May 2026, a month before Meta Glasses were released to the public.

100. That patent application—filed by Meta and titled "User Identity Verification without Sharing Biometric Data With Platforms"—describes in detail a facial-recognition and identity-verification system that mirrors the functionality publicly reported for Meta's NameTag technology.[38]

101. The patent application explains how a device, including "smart glasses," can capture images or videos of a person's face, generate biometric face embeddings from those images using a face-recognition algorithm, and compare those embeddings against face embeddings derived from profile photographs, tagged photographs, videos, or other images *already possessed by Meta's systems*.

102. The patent further describes machine-learning models trained on users' faces, the generation of face embeddings from both newly captured images and stored profile

[38] U.S. Patent Publication No. 20260142974 A1 (published May 21, 2026), *available by searching for "20260142974" at* https://ppubs.uspto.gov/basic/.

images, and a matching process designed to determine whether the captured individual is the same person represented in Meta's stored data.

103. Although the patent emphasizes a privacy-preserving architecture in which certain biometric embeddings need not be transmitted from the user's device to Meta's servers, the patent nevertheless confirms that Meta has developed and sought patent protection for technology capable of extracting facial biometric identifiers from images captured by smart-glasses devices and matching those biometric identifiers against biometrics **already in Meta's possession**. The patent therefore provides a detailed technical blueprint for precisely the type of facial-recognition system that reports have described as "NameTag."

104. The patent is particularly significant because it does not describe a hypothetical or generic computer-vision concept. Rather, it discloses a complete operational workflow involving smart-glasses devices, cameras, face-detection and face-embedding algorithms, machine-learning models trained on faces, profile-photo matching, and identity verification against user accounts.

105. Meta's own patent filing demonstrates that Meta had designed and implemented the core technical components necessary to identify real-world individuals from images captured by Meta smart glasses and to compare those individuals against photographs and facial data **associated with Meta platform accounts**.

106. Upon information and belief, Meta not only collected biometrics from the images of people's Facebook and Instagram for use by NameTag during the inference stage, but also to train and test the facial-recognition model used by NameTag. Indeed, this is almost a certainty given that (1) Meta has repeatedly stated that user-generated content on

its platform is used to train its AI models, (2) Meta has boasted about its "data advantage" in terms of training data as "the public images that have been shared on Facebook and Instagram,"[39] and (3) the biometric data used by NameTag for facial recognition comes from Facebook and Instagram photos.

107. Meta's covert collection, storage, and use of biometric data from images uploaded to platforms such as Facebook and Instagram poses a serious threat to privacy and civil liberties, and violates the laws of both Illinois and California.

108. Specifically, Meta's collection, storage, and use of these biometric identifiers is a violation of the Illinois Biometric Information Privacy Act, as Meta:

(a) does not provide the public with a written policy specifying the retention of its users' biometric information, as required by § 15(a) of BIPA; and

(b) does not provide written notice—or obtain informed written consent from users—of its collection and storage of biometric identifiers, as required by § 15(b).

109. By covertly collecting, storing, using, and profiting from images uploaded to its platforms—such as Facebook and Instagram—and the biometric identifiers obtained from those images, Meta is also violating individuals' right to publicity under California common law, misappropriating their likenesses in violation of California Civil Code § 3344(a), and invading their privacy in violation of the California Constitution.

[39] *Meta's Cox on Building AI Into the Product Suite*, at 6:09–7:01 (BLOOMBERG, May 9, 2024), https://www.bloomberg.com/news/videos/2024-05-09/meta-s-cox-on-building-ai-into-the-product-suite-video.

B. Generative AI: A new front in Meta's war on privacy.

110. While privacy and civil-liberties organizations have taken note of Meta's preparations and plans to release NameTag on the public, the issue of Meta's collecting and storing biometric data through its generative AI models has thus far been overlooked, in part because current GenAI is a relatively new technology, with its abilities and implications a topic of ongoing study and debate.

111. The information that is publicly available, however, is sufficient to reveal that Meta has used billions of images uploaded to platforms such as Facebook and Instagram to train its generative AI models—and that those same AI models extract and store biometric identifiers and information from both the images used in training and the images submitted to the models during the inference stage, when a user prompts the model.

1. Meta pivots from the "metaverse" to AI.

112. Meta was a latecomer to the world of consumer-facing generative AI, announcing its first consumer AI products in September 2023, nearly a year after the public debut of ChatGPT:

> We're introducing Meta AI in beta, an advanced conversational assistant that's available on WhatsApp, Messenger, and Instagram, and is coming to Ray-Ban Meta smart glasses and Quest 3. Meta AI can give you real-time information and generate photorealistic images from your text prompts in seconds to share with friends.
>
> …
>
> Soon, you'll be able to transform your images or even co-create AI-generated images with friends. Restyle and backdrop—two new features that are coming soon to Instagram—use the technology from

> Emu. Backdrop also leverages learnings from our Segment Anything Model.[40]

113. Meta's late entrance into the world of consumer-facing GenAI was largely a byproduct of the company's massive investment in the "metaverse"—3D digital spaces known as "Horizon Worlds," where people interacted through digital avatars while wearing virtual-reality headsets.

114. Launched in 2021, Horizon Worlds was mostly abandoned by 2026, as the platform never drew more than a few hundred thousand monthly active users and accumulated nearly $80 billion in losses for Meta.[41]

115. Just as it had with its failed metaverse project, once Meta decided that it wanted to dominate the GenAI industry, the company went all-in.

116. Meta "tried to poach OpenAI employees by offering signing bonuses as high as $100 million,"[42] with "pay packages of up to $300 million over four years."[43]

117. As the New York Times described it in the summer of 2025: "Silicon Valley's A.I. talent wars have become so frenzied—and so outlandish—that they increasingly

---

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

[41] Jackie Snow, *Meta is killing off the metaverse. It lost $80 billion*, QUARTZ (Mar. 18, 2026), https://qz.com/meta-metaverse-mark-zuckerberg-horizon-worlds-ai.

[42] Dylan Butts, *Sam Altman says Meta offered OpenAI staff $100 million bonuses, as Mark Zuckerberg ramps up AI poaching efforts*, CNBC (June 18, 2025), https://www.cnbc.com/2025/06/18/sam-altman-says-meta-tried-to-poach-openai-staff-with-100-million-bonuses-mark-zuckerberg.html.

[43] Zoë Schiffer, *Here's What Mark Zuckerberg is Offering Top AI Talent*, WIRED (July 1, 2025), https://www.wired.com/story/mark-zuckerberg-meta-offer-top-ai-talent-300-million/.

resemble the stratospheric market for N.B.A. stars."[44] Meanwhile, Meta CEO Mark Zuckerberg confirmed that "Meta planned to continue throwing money at A.I. talent 'because we have conviction that superintelligence is going to improve every aspect of what we do.'"[45]

118. Over the past three years, Meta has released at least a dozen consumer-facing GenAI products, powered by increasingly powerful AI models. The following is a partial list:

Consumer Product	Release Date	Underlying Models
Meta AI	September 2023	Custom Llama 2-based assistant; later Llama 3/4
AI Stickers	September 2023	Llama 2 and Emu
Restyle	September 2023	Emu
Backdrop	September 2023	Emu
AI Characters	September 2023	Llama-family models
Imagine (chat image generation)	September 2023	Emu
Imagine with Meta AI website	December 2023	Emu
AI Studio	2024	Llama-family models
Movie Gen	October 2024	Movie Gen Video, Movie Gen Audio, Movie Gen Edit, and Movie Gen Personalized Video
Meta AI standalone app	2025	Llama-family models (later generations)
Muse Image	2026	Muse Image
Muse Video	2026	Muse Video

[44] Mike Isaac, et al, *A.I. Researchers Are Negotiating $250 Million Pay Packages. Just Like N.B.A. Stars*, THE NEW YORK TIMES (updated Aug. 1, 2025), https://www.nytimes.com/2025/07/31/technology/ai-researchers-nba-stars.html.

[45] *Id.*

2. Meta's text-to-image generative AI models and products.

119. Most relevant to this action are the text-to-image generative-AI models released by Meta, including (1) the **Emu** model, used to generate images for Meta products such as Imagine, AI Stickers, Restyle, Backdrop, and Meta AI, Instagram AI, and WhatsApp image generation; and (2) the **Muse Image** model, which replaced the Emu model for image generation in mid-2026 for Meta products such as Meta AI, Instagram AI, and WhatsApp AI.

120. A text-to-image generative AI model is simply an AI model that takes a written description as input and generates a new image that matches the content of that description.

121. The Emu (Expressive Media Universe) AI model was Meta's flagship text-to-image model, unveiled by Meta in September 2023 and used as the foundation for several consumer image-generation features across products.

122. Emu is what is known as a latent diffusion model, which is a type of AI model that learns to create realistic images by starting with random noise and gradually turning that noise into a picture while working with compressed representations of images—sets of numbers that capture important information about an image while discarding non-essential information—to make the process faster and more efficient.[46]

[46] *Latent Diffusion Model: Definition & How It Works*, INFERENCE SYSTEMS (last visited Aug. 20, 2026), https://inferensys.com/glossary/synthetic-data-generation/text-to-image-generation/latent-diffusion-model.

123. Meta created Emu by first training a latent diffusion image-generation model on **1.1 billion image-text pairs** that were "internal" to Meta.[47] This step is referred to as "pre-training."

124. An image-text pair is simply an image together with text that describes, captions, labels or is otherwise associated with that image. An example of an image-text pair could be a Facebook photo of a birthday party paired with the text "Jane's 10th birthday party."

125. Meta then fine-tuned the model by using a few thousand "exceptionally high-quality images and associated text" to make the outputs more visually appealing—a process that Meta refers to as "post pre-training aesthetic alignment."[48]

126. Meta ultimately released at least three distinct Emu-based models: (1) Emu, the original text-to-image foundation model; (2) Emu Edit, an instruction-based image-editing model built on the Emu foundation model; and (3) Emu Edit, an instruction-based image-editing model built on the Emu foundation model.[49]

127. In May 2024, Meta's chief product officer, Chris Cox, publicly confirmed that Meta had used "photos and text from the platforms [Facebook and Instagram] to train its text-to-image generator model called Emu."[50]

---

[47] Xiaoliang Dai, et al., *Emu: Enhancing Image Generation Models Using Photogenic Needles in a Haystack* at 1–2, 5, ARXIV (Sept. 27, 2023), https://arxiv.org/pdf/2309.15807.

[48] *Id.*

[49] Anthony Alford, *Meta Announces Generative AI Models Emu Video and Emu Edit*, INFOQ (Nov. 28, 2023), https://www.infoq.com/news/2023/11/meta-emu-ai/.

[50] Jyotti Mann, *Meta is using your Instagram and Facebook photos to train its AI models*, YAHOO TECH (May 11, 2024), https://tech.yahoo.com/ai/articles/meta-using-instagram-facebook-photos-083101347.html.

128. Three years after its release of Emu, Meta released a new text-to-image model called Muse Image, available through the Meta AI app, Instagram, and WhatsApp.[51]

129. As soon as Muse Image was released on July 7, 2026, it was "already causing controversy":

> [A] particularly eyebrow-raising feature allows users to manipulate another Instagram user's images with AI, as long as that user's profile is public. Users merely tag the person, and it allows them to take their picture and use it to create a new AI image.
>
> Said one X user after The Verge first pointed out how potentially invasive this is: "Pulling real users into generated photos without explicit consent is a privacy landmine waiting to detonate."[52]

130. In response to the public backlash, Meta withdrew the Muse Image feature from Instagram only a few days after launch:

> "Earlier this week, we announced that one way for people to generate images in Meta AI is by @-mentioning public Instagram accounts that they want to reference," Meta said in a blog post. "Our intent was to provide a useful creative tool and to give people control over whether their public content could be referenced in this way. We've heard the feedback that this feature missed the mark, so it's no longer available."[53]

131. As with so many of Meta's apologies and statements over the past 20 years, its actions were meant to pacify the public while effectively changing nothing.

---

[51] Lucas Ropek, *Meta just launched a new AI generator, Muse Image, and users are already pushing back over use of their photos*, TECHCRUNCH (July 7, 2026), https://techcrunch.com/2026/07/07/meta-rolls-out-muse-a-new-ai-image-generator/.

[52] *Id.*

[53] Wendy Lee, *Meta discontinues Instagram feature on new AI image generation tool after Hollywood backlash*, LOS ANGELES TIMES (July 10, 2026), https://www.latimes.com/entertainment-arts/business/story/2026-07-09/meta-muse-image-ai-hollywood.

132. While Meta did remove the ability to "generate images in Meta AI is by @-mentioning public Instagram accounts" from *Instagram*, any member of the public could still do exactly the same thing using the Meta AI website (meta.ai) or the Meta AI app.

3. Meta's use of Facebook and Instagram images to train and test its text-to-image GenAI models results in the creation and storage of biometric identifiers and information within the models themselves.

133. It is public knowledge that Meta used at least **1.2 billion** image-text pairs—including image-text pairs obtained from Facebook and Instagram accounts—to train its Emu model.

134. In a article ironically titled "Privacy Matters," Meta stated that posts from Instagram and Facebook, including photos and text, were used to train the models behind its "new generative AI features."[54]

135. While Meta has not disclosed exactly how many such image-text pairs it has used to train its more recent text-to-image GenAI models, such as Muse Image, the statements from Meta's own online "Privacy Center" indicate that the company has used **billions** of its users' images for such training:

> Models that generate images: These models are trained by looking at **billions of images and their text captions**, which are the descriptive text associated with the images. **The model learns the association between these text descriptions and the images**. Once it's learned the association, it can create new images, like when a person enters a text description of the image they want generated.[55]

---

[54] Mike Clark, *Privacy Matters: Meta's Generative AI Features*, FACEBOOK (Sept. 27, 2023), https://about.fb.com/news/2023/09/privacy-matters-metas-generative-ai-features/.

[55] *How Meta uses information for generative AI models and features*, META (Aug. 20, 2026) (emphasis added), https://www.facebook.com/privacy/genai/.

136. Meta further states that because "it takes such a large amount of data to teach effective models," the company uses "a combination of sources" for training, including "**[i]nformation shared on Meta Products including things like posts or photos and their captions, and your interactions with features that are part of AI at Meta**."[56]

137. Moreover, when Meta "collect[s] training data to train [its] models," that data "may include **personal information**" such as the **name and contact information** of a blog's author and "**images of individuals**."[57]

138. Meta makes clear that it may use images of you even if you do *not* use one of Meta's platforms:

> Even if you don't use our Products or have an account, we may still process information about you to develop and improve AI at Meta. For example, this could happen if you appear anywhere in an image shared on our Products by someone who does use them or if someone mentions information about you in posts or captions that they share on our Products.[58]

139. Once trained, the AI model retains information about training data collected from Facebook and Instagram *even if a user deletes the information*:

> Models learn about patterns between pieces of information. **If you delete a piece of information a model learned from (like a public post), the model won't change in that moment.** However, your information itself will be deleted, and once it's deleted, it won't be used for future training.[59]

---

[56] *Id.* (emphasis added).

[57] *Id.*

[58] *Id.*

[59] *How generative AI models work*, META (Aug. 20, 2026) (emphasis added), https://www.facebook.com/privacy/dialog/how-generative-ai-models-work.

140. Meta's admissions regarding its harvesting of training data from Facebook and Instagram is significant because, during the training phase, Meta's text-to-image GenAI models transform the training images into numerical parameters and internal representations from which the model can later generate or reconstruct visual features.

141. Thus, when a training image contains a person's face, the model analyzes the person's facial features and generates numerical representations of the analyzed face.

142. These compact numerical features that represent facial identity are biometric identifiers or information—namely, scans of face geometry that can be used to identify a person.[60]

143. Meta has repeatedly suggested that its GenAI models do *not* memorize training data, stating for example that "[g]enerative AI is not a database or static collection of information."[61]

144. In litigation, Meta has even gone so far as saying of its large language model (LLM) called Llama, which generates text rather than images, that "nothing of the training data itself remains."[62]

[60] *How Meta uses information for generative AI models and features*, META (Aug. 21, 2026), https://www.facebook.com/privacy/genai/.

[61] *Id.*

[62] Def. Meta Platform Inc.'s Notice of Mot. and Mot. for Partial Summ. J., and Opp'n to Pls.' Mot. for Partial Summ. J. at 10, *Kadrey v. Meta Platforms, Inc.*, 3:23-cv-03417-VC-TSH (Mar. 24, 2025), Dkt. No. 501.

145. Meta's representation was conclusively disproven by researchers, who found that some training data "*are* 'memorized' by the model—encoded in some form inside the LLM's weights."[63]

146. Specifically, the researchers showed that LLMs— especially Meta's Llama model—memorize significant portions of their training data:

- "For instance, **LLAMA 3.1 70B entirely memorizes some books**, like *Harry Potter and the Sorcerer's Stone*; **memorization is so extensive that one can deterministically extract the whole book almost verbatim** using the book's first few words as an initial prompt."[64]
- "Extraction generates a 'copy' of training data, but **it also demonstrates that training data is memorized inside the model itself**."[65]
- "**LLAMA 3.1 70B memorizes some books, like *Harry Potter and the Sorcerer's Stone*** (hereafter, "*Harry Potter*") **and *1984*, almost entirely**. In fact, ***Harry Potter* is so memorized that one can deterministically extract a near-perfect copy of the book**, using an initial prompt consisting of just the first few words of the first chapter … ."[66]
- "[B]ooks like *Beloved* and *Kitchen Table Wisdom* represent a more intermediate case. For these books, memorization is generally low for most LLMs with respect to 50-token prefixes. **However, LLAMA 3 and LLAMA 3.1 70B memorize a considerable number of sequences, and increasing prefix length can sometimes reveal significant amounts of memorization.** For *Beloved*, 800-token

[63] A. Feder Cooper, et al., *Extracting memorized pieces of (copyrighted) books from open-weight language models* at 1, ARXIV (July 20, 2026) (emphasis added), *available at* https://arxiv.org/pdf/2505.12546.

[64] *Id.* at 1 (emphasis added).

[65] *Id.* at 2 (emphasis added).

[66] *Id.* at 2 (emphasis added).

prefixes reveal extraction coverage of **nearly 80% from LLAMA 3.1 70B** … ."[67]

- "[A]t least some LLMs (e.g., **LLAMA 3.1 70B**) may be derivative works of at least some books (e.g., *Harry Potter and the Sorcerer's Stone*)—because **those LLMs have memorized a significant amount of protectable expression from those books**."[68]

147. Significantly, LLMs are not the only generative AI models that memorize training data. The same is true of text-to-image models like Meta's Emu and Muse Image.

148. As early as 2023, researchers showed that image-generation models that, like Meta's Emu and Muse Image, are diffusion-based or diffusion-derived memorize individual training images and are therefore able to generate near-identical replicas of those images, including photographs of identifiable people:[69]

Figure 1: Diffusion models memorize individual training examples and generate them at test time. **Left:** an image from Stable Diffusion's training set (licensed CC BY-SA 3.0, see [49]). **Right:** a Stable Diffusion generation when prompted with "Ann Graham Lotz". The reconstruction is nearly identical (ℓ_2 distance = 0.031).

[67] *Id.* at 12 (emphasis added).

[68] *Id.* at 15 (emphasis added).

[69] Nicholas Carlini, et al., *Extracting Training Data from Diffusion Models* at 1, ARXIV (Jan. 30, 2023), https://arxiv.org/pdf/2301.13188.

149. This research "demonstrate[s] that state-of-the-art diffusion models *do* memorize and regenerate individual training examples"—including images of people's faces.[70]

150. Noting that "[t]raining data extraction attacks can present a threat to user privacy,"[71] the researchers "focus[ed] on worst-case privacy under a much more restrictive notion of memorization, and perform[ed] [their] attacks on a wider range of models."[72]

151. In the conclusion of their paper, the researchers note that their findings raise significant legal, ethical, and privacy issues:

> **State-of-the-art diffusion models memorize and regenerate individual training images, allowing adversaries to launch training data extraction attacks.** By training our own models we find that increasing utility can degrade privacy, and simple defenses such as deduplication are insufficient to completely address the memorization challenge. We see that state-of-the-art diffusion models memorize 2× more than comparable GANs, and more useful diffusion models memorize more than weaker diffusion models. **This suggests that the vulnerability of generative image models may grow over time.** Going forward, our work raises questions around the memorization and generalization capabilities of diffusion models.
>
> …
>
> On the whole, **our work contributes to a growing body of literature that raises questions regarding the legal, ethical, and privacy issues that arise from training on web-scraped public data**. Researchers and practitioners should be wary of training on uncurated public data without

[70] *Id.*

[71] *Id.* at 3.

[72] *Id.* at 2.

> first taking steps to understand the underlying ethics and privacy implications.[73]

152. This research demonstrates that text-to-image generative AI models such as Meta's Emu and Muse Image store mathematically encoded facial characteristics from training data that are sufficient to instantiate, reproduce, or identify the underlying individual.

153. Despite the model-retained data being stored in compressed latent form rather than as face embeddings that are utilized by traditional face-recognition models, these data are biometric identifiers and biometric information because these data can be used to recognize an image of a person's face and even to *reproduce* it.

154. This occurs because, when Meta trains a generative-AI model on a photograph containing a person's face, Meta's systems detect, encode, and preserve measurements and relationships among identity-relevant facial features in model parameters, embeddings, latent representations, feature vectors, or materially equivalent numerical representations.[74]

---

[73] *Id.* at 15 (emphasis added).

[74] *See, e.g.*, Michael Fuest, et al., *Diffusion Models and Representation Learning: A Survey* at 1, ARXIV (June 30, 2024) ("The remarkable generative capabilities of Diffusion Models suggest that Diffusion Models learn both low and high-level features of their input data, potentially making them well-suited for general representation learning."), *available at* https://arxiv.org/pdf/2407.00783v1.

155. Meta's Gen AI model Emu, for example, "has an autoencoder (AE) to encode an image to latent embeddings."[75]

156. Those identity-specific numerical representations are not photographs. They are scans and measurements of facial features capable of representing, distinguishing, reproducing, or identifying the depicted person.

157. In sum, Meta has collected, stored, and used Facebook and Instagram images depicting Plaintiffs' and Class Members' faces as training data for its text-to-image GenAI models, including but not limited to the Emu and Muse Image models, resulting in those models' memorization of biometric identifiers and information—regardless of whether or not the depicted person uploaded the image, maintained a Meta account, or knew that the image would be used for training Meta's GenAI models.

4. When a user submits an image of a person's face to one of Meta's text-to-image GenAI models via prompting (the inference stage), the model likewise creates and stores a biometric identifier of biometric information associated with the person in the image.

158. Meta's GenAI models do not create and store biometric identifiers and information only during training. When a user submits an image of a person to one of Meta's publicly available GenAI models as part of a prompt—known as the inference stage—the model analyzes features in the photo and generates and stores numerical

[75] Xiaoliang Dai, et al., *Emu: Enhancing Image Generation Models Using Photogenic Needles in a Haystack* at 1–2, 5, ARXIV (Sept. 27, 2023), https://arxiv.org/pdf/2309.15807. A latent embedding is a vector (series of numbers) in latent space. In machine learning, a latent space "is a compressed representation of data points that preserves only essential features that inform the input data's underlying structure." Dave Bergmann, *What is latent space?*, IBM (visited Sept. 2, 2026), https://www.ibm.com/think/topics/latent-space.

representations of the person's face that likewise can be used to identify the person and is therefore a biometric identifier or information under BIPA.

159. Meta states in its privacy policy that it "collect[s] and use[s]" information submitted to its generative AI products, including "questions, messages, **media and other information**."[76]

160. When a user provides an image containing a person's face to Meta AI, Muse Image, or another Meta generative-AI feature, Meta's systems detect and encode that face into an embedding, latent representation, feature vector, or materially equivalent numerical representation so the model can preserve, manipulate, or reproduce the person's identity by, for example, creating a deepfake.

161. Because the representation created by the model records identity-relevant facial measurements and can be used to generate an image of the same person or to recognize them, it constitutes a scan of face geometry and biometric identifier or information under BIPA.

162. In addition, when users submit images containing faces to Meta's GenAI during the inference stage via prompting, Meta uses those images to further train its GenAI models, resulting in the creation and storage of biometric identifiers and information described above.

[76] *Meta Privacy Policy*, FACEBOOK (Aug. 14, 2026) (emphasis added), https://www.facebook.com/privacy/policy/.

163. This is confirmed by Meta's own statements that its training data includes "interactions with features that are part of AI at Meta":[77]

> We use the information people share when interacting with our generative AI features, such as Meta AI or businesses who use generative AI, to improve our products and for other purposes.[78]

C. Meta profited from its collection and use of Plaintiffs' and Class Members' images and biometric data, and Plaintiffs and Class Members were injured by Meta's wrongful conduct.

164. Meta used images of Plaintiffs and Class Members as free raw materials for training and powering NameTag facial-recognition features as well as Meta's GenAI models such as Emu and Muse Image.

165. Meta used images of Plaintiffs and Class Members to train and test the facial-recognition model used by NameTag, generating biometric identifiers and biometric information in the process.

166. Once the model was trained, Meta stored Plaintiffs' and Class Members' biometric identifiers and information in a database for use by NameTag to identify people whose images were captured by Meta Glasses.

167. Meta profited from the above by, among other things, reducing development costs, improving product performance, increasing the value and marketability of Meta Glasses, strengthening the corporation's AI ecosystem, and generating present and

---

[77] *How Meta uses information for generative AI models and features*, META (accessed Aug. 21, 2026), https://www.facebook.com/privacy/genai?entry_point=POLICY_SUBPAGE%3Abanner.subpage.agentic-ai-2026-h1-eu.

[78] Mike Clark, *Privacy Matters: Meta's Generative AI Features*, FACEBOOK (Sept. 27, 2023), https://about.fb.com/news/2023/09/privacy-matters-metas-generative-ai-features/.

future revenue opportunities that would not have existed without Meta's possession and use of Plaintiffs' and Class Members' images and biometric data.

168. Meta also used images of Plaintiffs and Class Members to train its text-to-image GenAI models, including Emu and Muse Image—a process that resulted in those models storing Plaintiffs' and Class Members' biometric data.

169. Biometric data was also extracted and stored by Meta when images of Plaintiffs and Class Members were submitted to Meta's GenAI models during the inference stage (through prompting).

170. In short, Meta used Plaintiffs' and Class Members' images and biometric data to train, test, improve, evaluate, and continuously refine image-generation models such as Emu and Muse Image.

171. This use of Plaintiffs' and Class Members' images and biometric data profited Meta by reducing development costs, improving model performance, increasing user engagement, generating advertising and subscription revenue, strengthening Meta's competitive position in the generative-AI market, enhancing the value of its platforms, and increasing the value of the company itself.

172. As a direct and proximate result of Meta's unlawful conduct, Plaintiffs and Class Members have suffered concrete and particularized injuries and continue to face a substantial and ongoing risk of future harm.

173. By collecting, creating, analyzing, storing, using, disclosing, commercializing, and otherwise exploiting Plaintiffs' and Class Members' biometric identifiers, biometric information, photographs, likenesses, and related personal information without the notice, consent, disclosures, and safeguards required by law, Meta deprived Plaintiffs and Class

Members of their statutory and property rights in their personal information and of their ability to make informed decisions regarding the collection and use of their uniquely sensitive biometric data.

174. Plaintiffs and Class Members lost the opportunity to control, withhold, license, monetize, or otherwise determine how their biometric identifiers, face geometry, photographs, likenesses, and personal information would be collected and used.

175. Because biometric identifiers are unique and cannot be changed if compromised, the unauthorized collection, retention, dissemination, and commercialization of such information exposes Plaintiffs and Class Members to ongoing privacy harms, including the risk of unwanted identification, tracking, profiling, surveillance, impersonation, social engineering, identity theft, and other misuse.

176. Meta has derived substantial commercial, competitive, technological, and financial benefits from the use of Plaintiffs' and Class Members' information, including through the development, training, improvement, personalization, and commercialization of its products, algorithms, artificial intelligence systems, advertising technologies, and related business operations, while Plaintiffs and Class Members received no compensation and no meaningful opportunity to consent, object, or prevent such exploitation.

177. As a result, Plaintiffs and Class Members have suffered injury in fact, including invasion of privacy, loss of control over their biometric and personal information, misappropriation of their identities and likenesses, diminution in the value of their data, and the loss of the benefit of the bargain contemplated by applicable privacy and biometric-protection laws.

D. Delayed Discovery, Equitable Tolling, and Fraudulent Concealment.

178. Plaintiffs and Class Members did not discover, and through the exercise of reasonable diligence could not have discovered, the facts underlying their claims until mid-2026.

179. Meta's wrongful conduct involved proprietary facial-recognition systems, face embeddings, biometric matching technologies, machine-learning models, identity-verification systems, and related artificial-intelligence technologies that were maintained within Meta's internal systems and were not publicly disclosed in any meaningful manner. The existence, scope, operation, and use of those technologies were uniquely within Meta's knowledge and control.

180. Meta concealed material facts concerning both (a) its development and use of facial-recognition and identity-matching technologies and (b) its use of user-generated images and photographs—including its collection of biometric data from those images and photographs—in connection with generative-AI products and services.

181. Ordinary users had no reasonable means of determining the extent to which Meta could generate face embeddings from photographs and videos, match individuals to known identities, or utilize visual content within its Gen AI systems. Those facts resided within Meta's proprietary systems, source code, machine-learning models, internal databases, and confidential business records.

182. The first major set of disclosures regarding Meta's smart-glasses ecosystem and facial-recognition capabilities occurred in 2026.

183. Public reporting revealed that Meta had developed facial-recognition functionality reportedly known internally as "NameTag," that facial-recognition code had

been embedded within Meta software associated with its smart-glasses products, and that related systems were capable of detecting faces, generating biometric identifiers or face embeddings, and matching those identifiers against known profiles.

184. Those revelations were further corroborated by Meta's patent application, which describes systems capable of generating face embeddings from images and videos and comparing them to profile photographs and other stored facial imagery for identity verification purposes.

185. A second and separate set of disclosures concerning Meta's generative-AI products occurred in 2026.

186. Through Meta's public statements and reporting regarding products such as Muse Image, users learned that Meta's AI ecosystem was utilizing massive quantities of visual content and photographs associated with user accounts and public postings.

187. These disclosures provided users with the first meaningful visibility into the extent to which Meta's AI systems were being trained on or otherwise leveraging vast repositories of user-generated images and visual content.

188. Prior to the June 2026 revelations regarding NameTag, Plaintiffs had no reasonable basis to know that Meta had developed or was deploying facial-recognition and identity-matching technologies capable of extracting and comparing facial biometric information.

189. Likewise, prior to the July 2026 public backlash resulting from Meta's deployment of Muse Image features to Instagram, Plaintiffs had no reasonable basis to know the scope and manner in which Meta's AI systems utilized user photographs, visual content, and related data for AI development and operation.

190. Meta's concealment and nondisclosure prevented Plaintiffs and Class Members from discovering the factual basis of their claims despite the exercise of reasonable diligence.

191. Accordingly, the limitations period applicable to Plaintiffs' claims was tolled under the discovery rule, the doctrine of fraudulent concealment, and the doctrine of equitable tolling.

192. Thus, the limitations period did not begin to run until mid-2026, when Plaintiffs first discovered, or reasonably could have discovered, the facts giving rise to their claims through the foregoing 2026 disclosures concerning Meta's facial-recognition technologies, smart-glasses ecosystem, identity-verification systems, and generative-AI products.

193. Plaintiffs filed this action within a reasonable time thereafter, and all claims asserted herein are therefore timely.

V. CLASS ACTION ALLEGATIONS

194. Plaintiffs bring this action on behalf of themselves and under Federal Rule of Civil Procedure 23(a), (b)(2), and (b)(3), as representatives of the Classes defined as follows, subject to confirmation, clarification, or modification based on discovery to be conducted in this action:

> **The Illinois Class (For Claims 1 and 2 Under Illinois Law):**
>
> All persons in the State of Illinois whose image was uploaded to (1) a Facebook account, (2) an Instagram account, and/or (3) to any of Meta's generative AI models during the inference stage.

The National Class (For Claims 3 and 4 under California Law):

All persons in the United States whose image was uploaded to (1) a Facebook account, (2) an Instagram account, and/or (3) to any of Meta's generative AI models during the inference stage.

The California Class (For Claim 5 Under California Law and, in the alternative to the National Class, for Claims 3 and 4 under California Law):

All persons in the State of California whose image was uploaded to (1) a Facebook account, (2) an Instagram account, and/or (3) to any of Meta's generative AI models during the inference stage.

195. For purposes of this action, the Class Period is defined as September 4, 2021 through the present.

196. Excluded from the Classes are Defendant Meta and any entity in which Defendant has a controlling interest, as well as any of Defendant's legal representatives, officers, directors, assignees, and successors.

197. Members of the Classes are so numerous that joinder of all Class Members is impractical. Meta has publicly stated that it used 1.1 billion text-pair images to train its Emu model and has boasted about using its users' content to train its AI models in general. Given that there are over 250 million Facebook and over 160 million Instagram users in the United States, by conservative estimates, members of the National Class number in the millions and members of the Illinois and California Classes number in the hundreds of thousands. Class Members are readily identifiable from information and records in Meta's possession.

198. Plaintiffs' claims are typical of the claims of the members of the Class Members. Plaintiffs and Class Members were aggrieved by the same wrongful conduct of Meta alleged herein.

199. Plaintiffs will fairly and adequately protect and represent the interests of the Classes. The interests of Plaintiffs are coincident with, and not antagonistic to, those of the other members of the Classes.

200. Plaintiffs are represented by counsel with experience in the prosecution of class actions and with particular experience with class actions raising claims under BIPA and other privacy statutes.

201. Questions of law and fact common to the members of the Classes predominate over questions that may affect only individual Class Members because Meta has acted on grounds generally applicable to all of the Classes, thereby making damages with respect to the Class as a whole appropriate. Such generally applicable conduct is inherent in Meta's wrongful actions.

202. Questions of law and fact common to the Classes include:

a. Whether Meta engaged in the wrongful conduct alleged herein.

b. Whether Meta used images of Plaintiffs and Class Members to train the facial-recognition model utilized by NameTag.

c. Whether Meta used images of Plaintiffs and Class Members to test the facial-recognition model utilized by NameTag.

d. Whether Meta has stored numerical representations of Plaintiffs' and Class Members' faces for use by NameTag to identify persons whose images are captured by Meta Glasses.

e. Whether the data created by NameTag from images of Plaintiffs and Class Members is a biometric identifier or biometric information.

f. Whether Meta used images of Plaintiffs and Class Members to train its generative AI models, including but not limited to Emu and Muse Image.

g. Whether images of Plaintiffs and Class Members were submitted to Meta's generative AI models, including Emu and Muse Image, through prompting.

h. Whether the data created by Meta's generative AI models from images of Plaintiffs and Class Members—during either the training, testing, or inference stages—is a biometric identifier or biometric information.

i. Whether Meta adequately informed Plaintiffs and Class Members that it was collecting, storing, and using their biometric data.

j. Whether Meta properly obtained consent from Plaintiffs and Class Members for its collection, storage, and use of their biometric data.

k. Whether Meta's collection, storage, and use of Plaintiffs' and Class Members' biometric identifiers and biometric information collected was negligent, intentional, or reckless.

l. Whether Meta should be enjoined from collecting biometric identifiers and information through Facebook or Instagram, or through the information provided to its generative AI models by users during the inference stage.

203. Class-action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons or entities a method for obtaining redress on claims that could not practicably be pursued individually, substantially outweighs potential difficulties in management of this class action.

204. Plaintiffs know of no special difficulty to be encountered in the maintenance of this action that would preclude its maintenance as a class action.

VI. CLAIMS FOR RELIEF

CLAIM 1: Violation of Section 15(a) of the Illinois Biometric Information Privacy Act (by Plaintiffs Francisco Alvarez and I.W., a minor proceeding by and through his guardian Francisco Alvarez, on Behalf of Themselves and Members of the Illinois Class)

205. Plaintiffs repeat and incorporate by reference all preceding paragraphs and allegations.

206. Section 15(a) of BIPA provides that "[a] private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information … ."[79]

207. The biometric identifiers and information must be permanently destroyed "when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first."[80]

208. Meta is a Delaware corporation and is therefore a "private entity" under BIPA.[81]

209. The numerical representations of Plaintiffs' and Class Members' faces that were created by using their images during the training, testing, and inference stages of both

[79] 740 ILCS 14/15(a).

[80] 740 ILCS 14/15(a).

[81] 740 ILCS 14/10.

NameTag's facial-recognition model and Meta's GenAI models such as Emu and Muse Image are "biometric identifiers" and "biometric information" under BIPA.[82]

210. Meta did not properly develop or make publicly available a written policy governing the retention of the biometric identifiers and information collected from Plaintiffs and Class Members.

211. By improperly retaining the biometric data of Plaintiffs and Class Members, Meta violated the very privacy interests that BIPA was intended to protect.

212. On behalf of themselves and the Class, Plaintiffs seek:

(a) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Meta to develop and make publicly available a retention policy that complies with BIPA's § 15(a);[83]

(b) the greater of liquidated damages of $5,000 or actual damages for each of Meta's intentional or reckless violations of § 15(a);[84]

(c) the greater of liquidated damages of $1,000 or actual damages for each of Meta's negligent violations of § 15(a);[85] and

(d) reasonable attorneys' fees and costs, and other litigation expenses.[86]

[82] *Id.*

[83] 740 ILCS 14/20(4).

[84] 740 ILCS 14/20(2).

[85] 740 ILCS 14/20(1).

[86] 740 ILCS 14/20(3).

CLAIM 2: Violation of Section 15(b) of the Illinois Biometric Information Privacy Act Information Privacy Act (by Plaintiffs Francisco Alvarez and I.W., a minor proceeding by and through his guardian Francisco Alvarez, on Behalf of Themselves and Members of the Illinois Class)

213. Plaintiffs repeat and incorporate by reference all preceding paragraphs and allegations.

214. Section 15(b) of BIPA makes it unlawful for any private entity to:

> collect, capture, purchase, receive through trade, or otherwise obtain a person's … biometric identifier or biometric information, unless it first: (1) informs the subject … in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject … in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information … .[87]

215. The "written release" required by § 15(b)(3) means "informed written consent."[88]

216. Meta systematically collected, stored, and used Plaintiffs' and Class Members' biometric identifiers and information without providing the notice required by § 15(b)—including notice that their biometric data was being used for the "specific purposes" of (among other things) training and testing the facial-recognition model used by NameTag; identifying person's whose image is captured by Meta Glasses; and training Meta's GenAI models such as Emu and Muse Image.

217. Meta never obtained from Plaintiffs or Class Members the informed written consent required by BIPA.

---

[87] 740 ILCS 14/15(b).

[88] 740 ILCS 14/10.

218. By improperly collecting, storing, and using Plaintiffs' and Class Members' biometric identifiers and information, Meta violated their rights to privacy in their biometric data.

219. On behalf of themselves and the Class, Plaintiffs seek:

(a) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Meta to comply with § 15(b)'s requirement for collecting, storing, and using biometric identifiers and information;[89]

(b) the greater of liquidated damages of $5,000 or actual damages for each of Meta's intentional or reckless violations of § 15(b);[90]

(c) the greater of liquidated damages of $1,000 or actual damages for each of Meta's negligent violations of § 15(b);[91] and

(d) reasonable attorneys' fees and costs and other litigation expenses.[92]

CLAIM 3: Violation of California Common Law – Right of Publicity (by all Plaintiffs, on Behalf of Themselves and the National Class, and by Jeremy Wahl and I.W., a minor proceeding by and through her guardian Jeremy Wahl, on Behalf of Themselves and the California Class)

220. Plaintiffs repeat and incorporate by reference all preceding paragraphs and allegations.

221. California's common-law right of publicity protects a person from unauthorized use of their identity by another for commercial gain.

[89] 740 ILCS 14/20(4).

[90] 740 ILCS 14/20(2).

[91] 740 ILCS 14/20(1).

[92] 740 ILCS 14/20(3).

222. Meta knowingly used the identities, photographs, likenesses, and biometric data of Plaintiffs without authorization.

223. Meta obtained images of Plaintiffs and Class Members through Facebook, Instagram, and prompts submitted to Meta's generative-AI models, and (1) used those images to train and test NameTag and Meta's text-to-image GenAI models such as Emu and Muse Image; (2) generated and stored biometric data from those images, for use by both NameTag and Meta's GenAI models; and (3) used the images and associated biometric data for commercial gain or to otherwise benefit itself.

224. Meta appropriated Plaintiffs' and Class Members' identities, likenesses, facial characteristics, and biometrics for its own commercial advantage without authorization.

225. Rather than merely storing photographs, Meta extracted identity-related information from Plaintiffs' and Class Members' facial images, used those identity attributes to train and improve AI and facial-analysis systems, and incorporated the resulting capabilities into products and services from which Meta derives substantial economic benefit.

226. Plaintiffs and Class Members did not consent to the commercial exploitation of their identities, received no compensation for Meta's use of their biometrics, and suffered injury through the loss of exclusive control over the commercial value of their identities and the unauthorized appropriation of that value by Meta.

227. Use of the identities, photographs, likenesses, and biometric data of Plaintiffs and Class Members is directly connected to Meta's commercial activity.

228. Meta's unlawful conduct has harmed Plaintiffs and Class Members, and Meta has never compensated Plaintiffs or Class Members for the use of their identities, photographs, likenesses, and biometric data.

229. As a direct and proximate result of Meta's misconduct, Plaintiffs and Class Members have suffered harm and are entitled to monetary damages in an amount to be determined at trial.

230. Plaintiffs and Class Members also seek injunctive relief and such other equitable or declaratory relief as may be appropriate.

CLAIM 4: Violation of California Civil Code § 3344(a) – Commercial Misappropriation (by all Plaintiffs, on Behalf of Themselves and the National Class, and by Jeremy Wahl and I.W., a minor proceeding by and through her guardian Jeremy Wahl, on Behalf of Themselves and the California Class)

231. Plaintiffs repeat and incorporate by reference all preceding paragraphs and allegations.

232. California Civil Code § 3344(a) makes it unlawful for any person to knowingly "use[ ] another's name, voice, signature, photograph, or likeness, in any manner, on or in products, merchandise, or goods, or for purposes of advertising or selling, or soliciting purchases of, products, merchandise, goods, or services, without that person's prior consent, or, in the case of a minor, the prior consent of their parent or legal guardian … ."

233. Any person or entity who violates § 3344(a) is "liable to the injured party or parties in an amount equal to the greater of seven hundred fifty dollars ($750) or the actual damages suffered by them as a result of the unauthorized use, and any profits from the

unauthorized use that are attributable to the use and are not taken into account in computing the actual damages." Cal. Civ. Code § 3344(a).

234. Meta violated § 3344(a) by knowingly using the images, likenesses, and biometric identifiers of Plaintiffs and Class Members without obtaining their prior consent.

235. Specifically, Meta obtained images of Plaintiffs and Class Members obtained through Facebook, Instagram, and prompts submitted to Meta's generative AI models, and (1) used those images to train and test NameTag and Meta's text-to-image GenAI models such as Emu and Muse Image; (2) generated and stored biometric data from those images, for use by both NameTag and Meta's GenAI models; and (3) used the images and associated biometric data for commercial gain.

236. Meta knowingly used Plaintiffs' and Class Members' photographs, facial images, likenesses, biometric identifiers, and identity-related attributes for advertising, product development, artificial-intelligence training, identity-recognition functions, personalization systems, and other commercial purposes without first obtaining their consent.

237. Meta's use was directly connected to its revenue-generating business activities because the value of Meta's AI products, recommendation systems, advertising platform, identity-recognition technologies, and related commercial offerings depended in part upon the facial and identity information extracted from images of Plaintiffs and Class Members.

238. By appropriating Plaintiffs' and Class Members' identities and likenesses to develop, improve, market, and monetize those products and services, Meta obtained commercial benefits and profits attributable to that unauthorized use, entitling Plaintiffs and

Class Members to statutory damages, actual damages, disgorgement of profits, costs, and attorneys' fees under California Civil Code § 3344.

239. Meta's use of Plaintiffs' and Class Members' images, likenesses, and biometric data did not have any connection with the news, public affairs, sports broadcast or account, or any political campaign.

240. Plaintiff and Class Members have been harmed by Meta's conduct and are entitled to their actual or statutory damages.

241. Plaintiffs and Class Members are also entitled to attorney's fees and costs. Cal. Civ. Code § 3344(a).

CLAIM 5: Violation of California Constitution – Right to Privacy (by Plaintiffs Jeremy Wahl and I.W., a minor proceeding by and through her guardian Jeremy Wahl, on Behalf of Themselves and the California Class)

242. Plaintiffs repeat and incorporate by reference all preceding paragraphs and allegations.

243. Plaintiffs' and Class Members' privacy interest is reflected in several laws, including California's common law right of publicity and California Civil Code § 3344(a).

244. Plaintiffs and Class Members possess a legally protected privacy interest in their biometric identifiers, facial geometry, facial embeddings, identity-linked facial representations, and other biometric information derived from their photographs and videos.

245. Unlike ordinary personal information, biometric characteristics are unique, immutable, and capable of identifying a person across platforms, locations, and time.

246. Plaintiffs and Class Members did not voluntarily disclose either their images or biometric identifiers to Meta for the purpose of training artificial-intelligence models,

developing facial-recognition capabilities, creating identity-linked datasets, or enabling automated identity analysis.

247. Accordingly, Plaintiffs and Class Members retained a substantial privacy interest in that information.

248. Plaintiffs and Class Members also maintained a reasonable expectation of privacy that Meta would not transform their photographs and videos into biometric templates, facial embeddings, faceprints, identity vectors, or other machine-readable representations capable of recognizing, classifying, tracking, reproducing, or inferring information about them.

249. A reasonable person who shares a photograph on a social-media platform does not expect that the platform will extract and retain biometric identifiers from that image for use in developing commercial artificial-intelligence systems, facial-recognition technologies, identity-matching systems, or related products and services.

250. Meta intentionally invaded the privacy of Plaintiffs and Class Members by collecting, extracting, creating, storing, aggregating, analyzing, and exploiting biometric information derived from Plaintiffs' and Class Members' facial images without their informed consent.

251. Meta further incorporated that information into AI and identity-recognition systems that derive substantial commercial value from the ability to recognize, model, analyze, and generate identity-related outputs.

252. The scope of the invasion was extensive because Meta collected and used biometric information from enormous numbers of user photographs and videos and retained those identity-linked representations for continuing technological and commercial purposes.

253. The intrusion was highly offensive to a reasonable person and constituted an egregious breach of social norms.

254. Plaintiffs and Class Members did not consent to the extraction and commercialization of biometric identifiers from their likenesses, did not receive compensation for such use, and were deprived of the ability to control how their biometric identities would be collected, retained, analyzed, disclosed, or exploited.

255. Because biometric identifiers are permanent and cannot be revoked or replaced if compromised, Meta's conduct exposed Plaintiffs and Class Members to ongoing risks of identification, tracking, profiling, surveillance, and future uses of their biometric identities that Plaintiffs and Class Members cannot fully know or control.

256. Plaintiffs and Class Members have suffered injuries as a result of Meta's wrongful conduct, and they are entitled to appropriate relief, including compensatory and punitive damages.

257. Unless and until Meta is enjoined and restrained by order of this Court from continuing its wrongful conduct, Meta will continue to cause great and irreparable injury to Plaintiffs and Class Members, as Meta and others continue to use the unlawfully obtained biometric data and other personal information to the detriment of Plaintiffs and Class Members.

258. Injunctive relief is necessary because Plaintiffs and Class Members have no adequate remedy at law for their injuries, as a judgment for monetary damages will not end the invasion of their privacy or require that Meta delete their biometric identifiers and other personal information in Meta's possession, custody, or control.

VII. PRAYER FOR RELIEF

259. WHEREFORE, on behalf of themselves and the Class, Plaintiffs respectfully request that this Court enter an Order:

a. Certifying this case as a class action under Federal Rule of Civil Procedure 23(a), (b)(2), and (b)(3) on behalf of the National Class defined above, appointing all Plaintiffs as representatives of the National Class, and appointing their counsel as Class Counsel;

b. Certifying this case as a class action under Federal Rule of Civil Procedure 23(a), (b)(2), and (b)(3) on behalf of the Illinois Class defined above, appointing Plaintiffs Francisco Alvarez and F.M.A. (a minor proceeding by and through his guardian Francisco Alvarez) as representatives of the Illinois Class, and appointing their counsel as Class Counsel;

c. Certifying this case as a class action under Federal Rule of Civil Procedure 23(a), (b)(2), and (b)(3) on behalf of the California Class; appointing Plaintiffs Jeremy Wahl and I.W. (a minor proceeding by and through her guardian Jeremy Wahl) as representatives of the California Class; and appointing their counsel as Class Counsel;

d. Declaring that Meta's actions, as set out above, violate § 15(a) and (b) of BIPA;

e. Awarding all Plaintiffs and members of the National and California Classes statutory, compensatory, punitive, exemplary, consequential, general, and nominal damages in an amount to be determined at trial;

f. Awarding Plaintiffs Francisco Alvarez, F.M.A., and Members of the Illinois Class the greater of actual damages or statutory damages of $5,000 per intentional or reckless violation of BIPA, and the greater of actual damages or statutory damages of $1,000 per negligent violation of the BIPA;

g. Granting permanent injunctive relief to prohibit Meta from continuing to engage in the unlawful acts and practices described herein;

h. Awarding Plaintiffs and Class Members their reasonable litigation expenses and attorneys' fees;

i. Awarding Plaintiffs and Class Members pre- and post-judgment interest, to the extent allowable; and

j. Awarding such other and further relief as equity and justice may require.

VIII. JURY DEMAND

260. Plaintiffs demand a trial by jury on all issues so triable.

Dated: September 4, 2026

/s/ Justin N. Boley

Kenneth Wexler
Justin N. Boley
Zoran Tasić
Gwyneth F. Lietz
WEXLER BOLEY & ELGERSMA LLP
311 S. Wacker Drive, Suite 5450
Chicago, IL 60606
Tel: (312) 346-2222
Fax: (312) 346-0022
kaw@wbe-llp.com
jnb@wbe-llp.com
zt@wbe-llp.com
gfl@wbe-llp.com

Ryan F. Stephan
James B. Zouras
Catherine Mitchell Duffy
Anna Ceragioli
STEPHAN ZOURAS, LLC
222 W. Adams St., Suite 2020
Chicago, Illinois 60606
Tel: (312) 233-1550
rstephan@stephanzouras.com
jzouras@stephanzouras.com
cmitchell@stephanzouras.com

aceragioli@stephanzouras.com

Daniel E. Gustafson
(*pro hac vice* forthcoming)
David A. Goodwin
(*pro hac vice* forthcoming)
Shashi K. Gowda
(*pro hac vice* forthcoming)
GUSTAFSON GLUEK PLLC
120 South Sixth Street, Suite 2600
Minneapolis, MN 55402
Tel: (612) 333-8844
dgustafson@gustafsongluek.com
dgoodwin@gustafsongluek.com
sgowda@gustafsongluek.com

Kevin Landau
(*pro hac vice* forthcoming)
Joshua Hall
(*pro hac vice* forthcoming)
TAUS, CEBULASH & LANDAU, LLP
123 William Street, Suite 1900A
New York, New York 10038
Tel: 646-873-7654
klandau@tcllaw.com
jhall@tcllaw.com

Attorneys for Plaintiffs and Proposed Class