Mike Arias (CSB #115385)
Elise R. Sanguinetti (CSB #191389)
Arnold C. Wang (CSB #204431)
Craig S. Momita (CSB #163347)
M. Anthony Jenkins (CSB #171958)
ARIAS SANGUINETTI WANG & TORRIJOS LLP
6701 Center Drive West, Suite 1400
Los Angeles, California 90045
Telephone: (310) 844-9696
Facsimile: (310) 861-0168
mike@aswtlawyers.com
arnold@aswtlawyers.com
craig@aswtlawyers.com
anthony@aswtlawyers.com

Thomas P. Rosenfeld (*pro hac vice* forthcoming)
Kevin P. Green (*pro hac vice* forthcoming)
Thomas C. Horscroft (*pro hac vice* forthcoming)
GOLDENBERG HELLER & ANTOGNOLI, P.C.
2227 South State Route 157
Edwardsville, Illinois 62025
Telephone: (618) 656-5150
tom@ghalaw.com
kevin@ghalaw.com
thorscroft@ghalaw.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

NATALIE TURCK, individually and on behalf of all others similarly situated, Plaintiff, v. META PLATFORMS, INC., a Delaware corporation, Defendant.	Case No: **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

TABLE OF CONTENTS

NOTICE TO DEFENDANT OF DUTIES TO RETAIN EVIDENCE:

TO DEFENDANT: Note and adhere to your duties to retain, and not delete or destroy, all documents, emails, databases, electronic records, electronically stored information, and all other evidence that may be pertinent to this lawsuit, and to cease any destruction or deletion of such evidence that might otherwise take place in the ordinary course of your business or affairs.

Plaintiff, Natalie Turck, on behalf of herself and all others similarly situated, for her Class Action Complaint against Defendant Meta Platforms, Inc. ("Meta"), states as follows upon personal knowledge as to herself and her own acts and experiences, and, as to all other matters, upon information and belief, including investigation conducted by her attorneys.

NATURE OF THE ACTION

1. This claim involves Illinois' Biometric Information Privacy Act, 740 ILCS 14/1 *et seq*. ("BIPA"), a law that regulates companies that possess, collect, capture, obtain, store, and use Illinois citizens' biometric data, such as voiceprints, fingerprints, and scans of face geometry, and information derived therefrom.

2. Meta owns and operates the social media platform, Facebook.

3. Meta also owns and operates Messenger, a messaging app that can be used for, *inter alia*, instant messages, sharing photos, videos, recording and sending audio recordings, group chats, and video and audio calls.

4. This case involves Meta's obtaining and possession of voiceprints and related biometric information from Illinois users of its Facebook and Messenger platforms in violation of BIPA.

5. Under BIPA, Meta may not collect, capture, purchase, receive through trade, or otherwise obtain a person's voiceprint unless it first obtained consent as set forth in BIPA §15(b),

which provides that, before a voiceprint or related biometric information (collectively "biometric data") is collected, captured, received through trade, or otherwise obtained, Meta is required to: (1) inform the person in writing that their biometric data is being collected or stored; (2) inform the person in writing of the specific purpose and length of term for which their biometric data is being collected, stored, and used; (3) receive a written release executed by the subject of the biometric data. 740 ILCS 14/15(b).

6. At least in 2023, and upon information and belief, for many years prior, Meta has been capturing, creating, collecting, and storing voiceprints and other related biometric information of Facebook and Messenger users from audio submitted via Facebook or Messenger.

7. Meta's maze of privacy policies nowhere accurately or fully describes its possession, capturing, collection, creating, obtaining, and use of voiceprints or other related biometric information. While Meta sought a patent in 2016 (issued in 2020) related to the use of voiceprints to identify users, which used the term "voiceprint" nearly 200 times, its disclosures to consumers nowhere uses the term.

8. Nor does Meta purport to seek any affirmative consent from users in advance of such capture, collection, creation, storage, and/or obtaining of voiceprints or related biometric information.

9. In fact, it was not until January 2023 that Meta updated its Privacy Policy to vaguely acknowledge that "[t]he categories of Personal Information we may have collected about you over the past 12 months," "may" have included "voice recordings" that "may be used to identify you."

10. That statement buried in Meta's website does not come close to satisfying the requirements of BIPA § 15(b).

11. Meta also lacks a retention and destruction policy for biometric data that complies with BIPA §15(a), which requires Meta to have a public written policy outlining that it will permanently destroy the biometric data once the initial purpose for its collection has been satisfied or within three years of the user's last interaction with Meta, whichever is earlier. 740 ILCS 14/15(a).

12. Instead, Meta's stated retention/destruction policy is to hold biometric data until it decides it no longer needs it: "We keep Personal Information, including sensitive Personal Information, as long as we need it to provide our products, comply with legal obligations or protect our or other's interests. We decide how long we need information on a case-by-case basis."

13. As a result of this "we decide" policy, Meta has unlawfully retained the biometric data of Plaintiff and the Class in violation of BIPA §15(a).

14. Meta also violates BIPA §15(c), which prohibits entities in possession of biometric data from selling, leasing, trading, or otherwise profiting from a person's biometric data. 740 ILCS 14/15(c). Meta profits off of the biometric data of Plaintiff and the Class in its possession by, *inter alia*, using the biometric data to improve its voice recognition and identification methods, software, processors, and machine learning; improve its products and product development for hardware and software that utilize voice recognition, such as user authentication features; and using biometric data to identify users so that it can send them customized, targeted content, including targeted advertisements.

15. At its core, Meta is a digital advertising company. As self-described in its most recent Annual Report filed with the United States Securities and Exchange Commission, "we generate substantially all of our revenue from selling advertising placements on our family of

apps to marketers . . . . Marketers purchase ads that can appear in multiple places including on Facebook, Instagram, Messenger, and third-party applications and websites."[1]

16. Meta also explained in its 2022 Annual Report that it was "making significant investments in artificial intelligence and machine learning to improve our delivery, targeting, and measurement capabilities" as a way of mitigating legislative and regulatory developments that have "impacted our ability to use data signals in our ad products."[2]

17. In 2022, Meta generated over $113.6 billion in advertising revenue alone, which constituted over 97% of Meta's total annual revenue. [3]

18. Ultimately, Meta profits from the biometric data of Plaintiff and the Class by, *inter alia*, using the biometric data to allow Meta to more effectively target users with ads and thus sell more of Meta's main product (targeted advertisements) to Meta's primary customers (advertisers).

19. Finally, Meta violates BIPA § 15(e), which requires entities in possession of biometric data to store, transmit, and protect from disclosure all biometric data using the reasonable standard of care in the industry and in a manner that is the same as or more protective than the manner in which the entity stores, transmits, and protects other confidential and sensitive information. 740 ILCS 14/15(e).

20. Meta's 2020 Annual Report explained that "[o]ur industry is prone to cyber-attacks by third parties seeking unauthorized access to our data or users' data," and further explained that "[a]s a result of our prominence, the size of our user base, the types and volume of personal data and content on our systems, and the evolving nature of our products and services

[1] Meta 2022 10-K, p. 7, https://www.sec.gov/Archives/edgar/data/1326801/000132680123000013/meta-20221231.htm.

[2] *Id.* p. 56.

[3] *Id.* p. 99.

(including our efforts involving new and emerging technologies), we believe that we are a particularly attractive target for such breaches and attacks . . . ."[4]

21. In September 2018, Meta announced the discovery of a third-party cyber-attack "that exploited a vulnerability in Facebook's code to steal user access tokens, which were then used to access certain profile information from approximately 29 million user accounts on Facebook."[5]

22. In the 2022 Annual Report, Meta stated: "[W]e have discovered and announced, and anticipate that we will continue to discover and announce, additional incidents of misuse of user data or other undesirable activity by third parties."

23. Meta further acknowledged that, because of factors such as its size and how it allocates its resources, it is simply unable to discover all intrusions into its user data by third parties: "We may not discover all such incidents or activity, whether as a result of our data or technical limitations, including our lack of visibility over our encrypted services, the scale of activity on our platform, the allocation of resources to other projects, or other factors, and we may be notified of such incidents or activity by the independent privacy assessor required under our modified consent order with the FTC, the media, or other third parties. Such incidents and activities have in the past, and may in the future, include the use of user data or our systems in a manner inconsistent with our terms, contracts or policies, the existence of false or undesirable user accounts, election interference, improper advertising practices, activities that threaten people's safety on- or offline, or instances of spamming, scraping, data harvesting, unsecured

[4] *Id.* p. 42.

[5] *Id.* p. 43.

datasets, or spreading misinformation. We may also be unsuccessful in our efforts to enforce our policies or otherwise remediate any such incidents."[6]

24. Accordingly, Plaintiff seeks to represent a class of similarly situated individuals to obtain an Order: (A) awarding Plaintiff and each Class Member statutory damages of $5,000 for each willful and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14.20(1); (B) enjoining Meta from possessing, collecting, obtaining, storing, using, selling, leasing, trading, and profiting from Plaintiff's and the Class Members' biometric data until done so in compliance with BIPA; (C) awarding Plaintiff and the Class Members reasonable attorneys' fees, costs, and other expenses pursuant to 740 ILCS 14/20(3); (D) awarding Plaintiff and the Class Members pre-and post-judgment interest, as provided by law; and (E) awarding such other and further relief as is just and appropriate.

PARTIES

25. Plaintiff is a natural person and citizen of the State of Illinois.

26. Meta is a Delaware corporation with its principal place of business in California. It is, therefore, a citizen of Delaware and California.

JURISDICTION AND VENUE

27. This Court has jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d). Because Plaintiff, who is a member of the Class, and Defendant are citizens of different States, there is minimal diversity. The total claims of Class Members exceed $5,000,000 exclusive of interest and costs. There are at least 100 Class Members.

28. This Court has personal jurisdiction over Defendant because it has its principal places of business in California and is, therefore, a citizen of California.

[6] *Id.*

29. Venue is proper in this district pursuant to 28 U.S.C. § 1391 because Defendant resides in this district and is a resident of the State in which this district is located.

COMMON FACTUAL ALLEGATIONS

I. Illinois' Protection of Biometric Data

30. The Illinois General Assembly enacted the Biometric Information Privacy Act, 740 ILCS 14/*et seq*. ("BIPA") in 2008 to establish standards of conduct for private entities that collect or possess biometric identifiers and biometric information.

31. "Biometric identifiers" covered by BIPA include retina or iris scans, fingerprints, voiceprints, and scans of human or face geometry. 740 ILCS 14/10.

32. "Biometric information" covered by BIPA includes "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." *Id.*

33. The Illinois General Assembly noted that BIPA was carefully crafted to protect biometric data because "unlike other unique identifiers that are used to access finances or other sensitive information," one's own biometric data cannot be changed; "[t]herefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." 740 ILCS 14/5.

34. The legislative findings also acknowledge that "[t]he full ramifications of biometric technology are not fully known." *Id.* § 14/5(f). Accordingly, the General Assembly found that "[t]he public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." *Id.* § 14/5(g).

35. The Seventh Circuit has also stated that biometric data is "meaningfully different" from other personal information, such as addresses, dates of birth, telephone numbers, and credit

card and social security numbers, because of the "inherent sensitivity of biometric data," which is "immutable, and once compromised, [is] compromised forever—as the legislative findings in BIPA reflect." *Fox v. Dakkota Integrated Sys., LLC*, 980 F.3d 1146, 1155 (7th Cir. 2020).

36. BIPA makes it unlawful for any private entity to, *inter alia*, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer'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 . . . ." 740 ILCS 14/15(b).

37. Furthermore, BIPA requires that any "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 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." 740 ILCS 14/15(a).

38. BIPA also provides that "[n]o private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information." 740 ILCS 14/15(c).

39. Finally, BIPA provides that "[a] private entity in possession of a biometric identifier or biometric information shall: (1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and (2) store, transmit, and protect from disclosure all biometric

identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information." 740 ILCS 14/15(e).

40. BIPA provides for a private right of action: "Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party." 740 ILCS 14/20.

41. The Illinois Supreme Court has explained that a person whose biometric identifiers are the subject of violations of section 15 of BIPA is "aggrieved" by the entity's failure to comply with BIPA and is "entitled to seek recovery" under Section 14/20. *Rosenbach v. Six Flags Entm't Corp*, 2019 IL 123186, ¶ 33 ("[W]hen a private entity fails to comply with one of section 15's requirements, that violation constitutes an invasion, impairment, or denial of the statutory rights of any person or customer whose biometric identifier or biometric information is subject to the breach. Consistent with the authority cited above, such a person or customer would clearly be 'aggrieved' within the meaning of section 20 of the Act (*id.* § 20) and entitled to seek recovery under that provision. No additional consequences need be pleaded or proved. The violation, in itself, is sufficient to support the individual's or customer's statutory cause of action.").

42. Under BIPA, "[a] prevailing party may recover ***for each violation***: (1) against a private entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater; (2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater; (3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and (4) other relief, including an injunction, as the State or federal court may deem appropriate." *Id.* (emphasis added).

II. Meta Repeatedly Chooses Self-Interest Over User Privacy Interests

43. Meta has a troubled history involving user privacy and the misuse of users' personal information, including biometric data.

44. Meta's practice seems to be to do whatever it needs to do to improve its products and bottom line, even if that conduct is at the expense of its users' privacy, and deal with privacy invasions after the fact.

45. In 2012, the Federal Trade Commission approved a Consent Order entered with Meta to resolve charges brought by the FTC that Facebook deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public. *See In re: Facebook, Inc.*, File No. 0923184 (FTC). The 2012 FTC Order required Meta to, *inter alia*, "not misrepresent in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information, including, but not limited to . . . its collection or disclosure of any covered information." *In re Facebook, Inc.*, C-4365, 2012 FTC LEXIS 135, *6 (F.T.C. July 27, 2012). "Covered information" meant "information from or about an individual consumer." *Id.* at *4.

46. In 2019, the United States filed a Complaint for Civil Penalties, Injunction, and Other Relief for Meta's violations of the 2012 FTC Order, seeking "to hold Facebook accountable for its failure to protect consumers' privacy as required by the 2012 Order and the FTC Act." *See United States v. Facebook, Inc.*, No. 1:19-cv-02184, ECF Dkt. 1, p. 1 (July 24, 2019).

47. The same day, Meta entered a Stipulated Order, in which it, *inter alia*, agreed to pay a civil penalty of $5,000,000,000. *Id.* ECF Dkt. 2-1, ECF p. 3. Meta also agreed to modify the 2012 FTC Order in numerous ways, one of which included specifically listing "biometric information" as an example of "information from or about an individual consumer" in the

definition of "covered information." *Id.* at ECF p. 11. The Modified Order also required Meta to delete any existing Facial Recognition Templates, clearly and conspicuously disclose in a stand-alone disclosure separate and apart from any privacy policy, data policy, or other similar page, how Meta would use and share facial recognition templates, and obtain affirmative express consent before creating any new facial recognition templates. *Id.* at ECF p. 16. Further, Meta agreed to internal procedures, safeguards, and reporting obligations related to the introduction of any "modified product, service, or practice that includes a material change in the collection, use, or sharing of Covered Information; a product, service, or practice directed to minors; or a product, service, or practice involving health, financial, biometric, or other similarly sensitive information." *Id.* at ECF pp. 17-19.[7]

48. On May 3, 2023, the FTC issued an Order to Show Cause alleging violations of the Modified 2012 FTC Order and seeking further modifications. *In re Facebook, Inc.*, File No. 2123091 (F.T.C.).

49. In addition to charges from the FTC, Meta has previously faced, and settled, civil litigation based on allegations that it allowed third parties, including Cambridge Analytica, to access users' personal information without consent. *See In re: Facebook, Inc. Consumer Privacy User Profile Litig.*, No. 3:18-md-02843-VC (N.D. Cal.).

50. Meta is currently facing civil litigation alleging that it has collected the health information of Facebook users from third parties without the users' consent. *See, e.g.*, *Doe v. Meta Platforms, Inc.*, No. 5:22-cv-03580-NC (N.D. Cal.).

[7] The Stipulated Order was entered by the United States District Court for the District of Columbia on April 23, 2020. *United States v. Facebook, Inc.*, 456 F. Supp. 3d 115 (D.D.C. 2020). Thereafter, the FTC entered its Order modifying the 2012 Order. *In re Facebook, Inc.*, 2020 FTC LEXIS 80, *4 (F.T.C. April 27, 2020).

51. Meta has previously settled, and faces continuing litigation, based on its obtaining scans of face geometry without consent in violation of BIPA and other similar state laws. *See In re: Facebook Biometric Info. Privacy Litig.*, No. 15-cv-03747-JD (N.D. Cal.); *Texas v. Meta Platforms, Inc.*, No. 22-0121 (Tex. Ct. [71st Dist.] 2022).

III. Beginning in 2016, Meta Seeks and Obtains Patent Protections for its System of Identifying Facebook Users with Voiceprints, with Updates in 2020, 2022, and 2023

52. In December 2016, Meta (then Facebook, Inc.) filed a patent application titled: "User Identification with Voiceprints on Online Social Networks."

53. Meta sought to protect methods, software, and processors for identifying users of its social network with voiceprints created from audio input into the social network site or related applications (e.g., an audio message sent by a Facebook user to another person via Messenger).

54. The patent was issued on March 31, 2020, Patent No. 10,607,148 (the "2020 Voiceprint Patent").

55. The 2020 Voiceprint Patent explained some of Meta's purposes for obtaining voiceprints, including, *inter alia*, (1) to identify users; (2) to associate voiceprints with unknown users; (3) to authenticate users; (4) and to identify users and provide the identified users with customized content.[8]

56. The 2020 Voiceprint Patent explained numerous uses for the methods, software, and processors protected by the patent, including how Meta can create voiceprints, use them to identify users, and store voiceprints:

> A social-networking system may record and analyze a user's voice to determine a digital voiceprint for the user. . . . The voiceprint may be received by a client system [e.g. a mobile device], stored on the social-networking system, and used to determine whether subsequently-received audio input is spoken by the same user. The social-networking system may use the voiceprint to identify or

[8] 2020 Voiceprint Patent, p. 4.

> authenticate a user based on audio input, and then perform actions based on voice commands in the audio input. . . . A voiceprint may be generated based on the audio input and stored in the data store as the user's voiceprint.[9]

57. In addition, the 2020 Voiceprint Patent explained that Meta can create and store voiceprints of its users when audio of them is received, not from the user, but from other sources (e.g., other users), and that Meta can utilize its vast data sources to link the voiceprint with a user:

> [T]he social-networking system may receive an audio input from an unknown user who is not associated with a voiceprint, and associate the audio input with a particular social-networking user and a probability that the audio input was spoken by the candidate user. A voiceprint may then be generated for the unknown user based on the audio input and associated with the candidate user and the probability. The candidate user and the probability may be identified by correlating where or when the audio input was received with the candidate user's social-networking information and information about any known users who may be connected to the candidate user in the social-networking system and/or located at or near the location of the candidate user.[10]

///

///

///

///

///

///

///

///

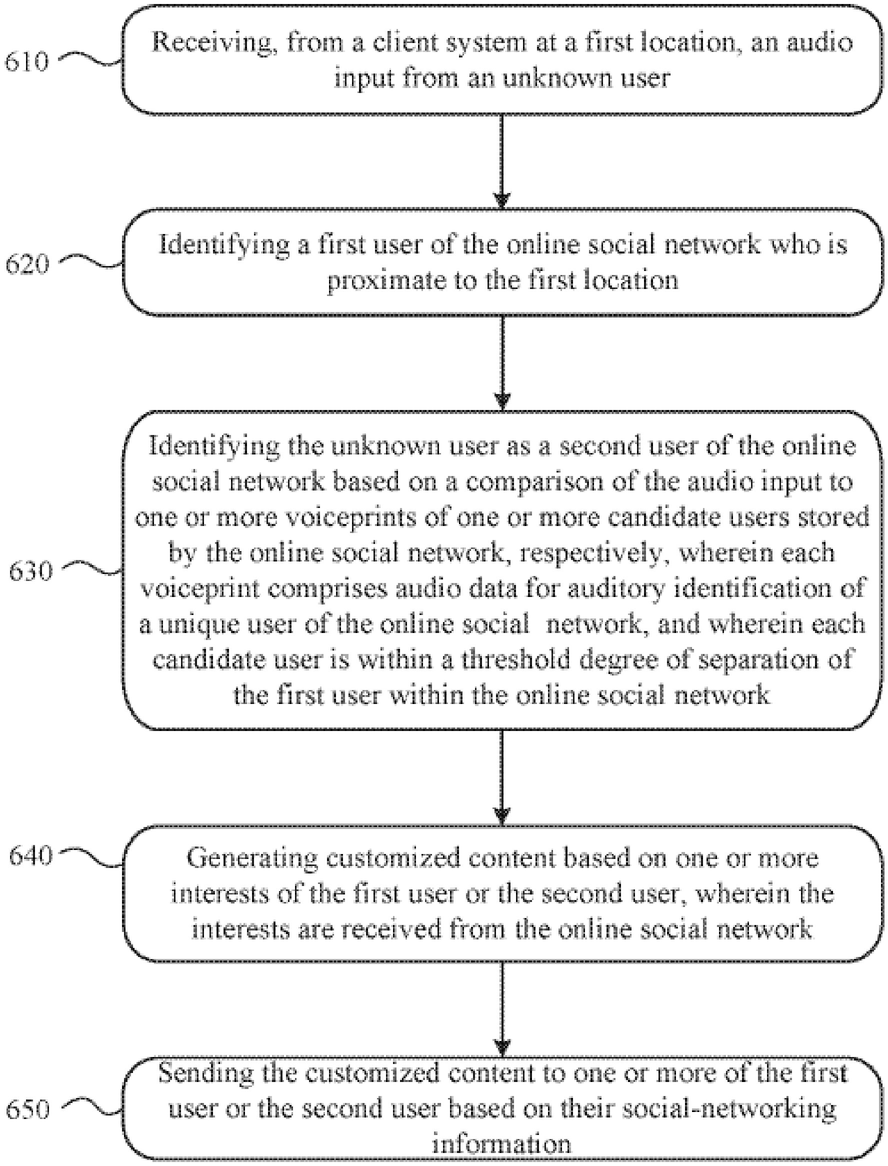
///

///

[9] *Id.* at 2.

[10] *Id.* at 3.

58. The 2020 Voiceprint Patent illustrates an example of providing customized content after voiceprint identification of an initially unknown user:[11]


610
Receiving, from a client system at a first location, an audio input from an unknown user
620
Identifying a first user of the online social network who is proximate to the first location
630
Identifying the unknown user as a second user of the online social network based on a comparison of the audio input to one or more voiceprints of one or more candidate users stored by the online social network, respectively, wherein each voiceprint comprises audio data for auditory identification of a unique user of the online social network, and wherein each candidate user is within a threshold degree of separation of the first user within the online social network
640
Generating customized content based on one or more interests of the first user or the second user, wherein the interests are received from the online social network
650
Sending the customized content to one or more of the first user or the second user based on their social-networking information

59. The 2020 Voiceprint Patent provided examples showing that "customized content" meant advertisements and other targeted content:

> A client device associated with the social-networking system may detect one or more people speaking, and the people speaking may be identified as users based on comparison of their voices to voiceprints stored by the social-networking system. Upon identifying one or more of the people as users of the social-

[11] *Id.* at Fig. 6.

> networking system, the social-networking system may provide customized content to the identified users based on their social-networking information. The customized content may be personalized to match the interests of the identified users, and may include advertisements, news feeds, push notifications, place tips, coupons, or suggestions.[12]

60. The 2020 Voiceprint Patent also explained that Meta may receive audio input from an unknown user, which it can compare to voiceprints of Facebook users to identify and target with customized content:

> [T]he social-networking system may receive, from a client system at a first location, an audio input from an unknown user. . . . [T]he social-networking system may identify a first user of the online social network who is proximate to the first location. As an example and not by way of limitation, the online social network may receive the identity of a user proximate to the first location by searching the known locations of users for locations that are within a threshold distance of the first location. The known locations of a user may be determined by the online social network based on the user's use of a client system that has sent its geographical location to the online social network, based on the user checking-in at the geographical location, based on identifying the user's voice at the geographical location via voiceprint analysis, or based on other techniques described herein. . . .
>
> [T]he social-networking system may identify the unknown user as a second user of the online social network based on a comparison of the audio input to one or more voiceprints of one or more candidate users stored by the online social network, respectively, wherein each voiceprint comprises audio data for auditory identification of a unique user of the online social network, and wherein each candidate user is within a threshold degree of separation of the first user within the online social network. . . .
>
> [T]he social-networking system may send customized content to one or more of the first user or the second user based on their social-networking information. . . . [T]he customized content may comprise content associated with the first location. . . . [T]he social-networking system may generate the customized content based on one or more interests of the first user or the second user, wherein the one or more interests are received from the online social network. . . . [T]he customized content may comprise content

[12] *Id.* at 32 (diagram numbers omitted).

> having one or more topics that match the interests of the first user or the second user. . . . [T]he customized content may comprise advertisements, news feeds, push notifications, place tips, coupons, suggestions, or a combination thereof.[13]

61. The 2020 Voiceprint Patent provided examples of how audio of multiple people can be captured from a device that is connected to a known (authenticated) Facebook user, which Meta can compare to stored voiceprints to identify the second person and push customized content to both:

> [W]hen multiple speakers are detected in audio input received by a client device of the social-networking system, the social-networking system may use voiceprint analysis to identify social network users who are connected to a known seed user, such as an authenticated user, e.g., the owner of a listening phone, and then send content to one or more of the social network users based on their interests. For example, suppose that two users, Marsha and Jan, are friends and are watching TV at Marsha's house. Marsha is an authenticated user of the TV at her house. A media device associated with the social-networking system (e.g., a dongle in communication with the TV) receives Jan's voice, and the social-networking system identifies Jan based on her voiceprint and on her social-graph connection to Marsha. Content or advertisements may then be provided to the users (e.g., to the TV, to Jan or Marsha's phone, etc.), and the content or advertisements may be customized to the interests of Marsha and Jan (e.g., the TV recommends a show or displays an advertisement for a product that both users are interested in). Content or advertisements may be provided to a group of three or more users if at least one of the users is an authenticated user.[14]

62. The 2020 Voiceprint Patent also provided examples of how audio of multiple people can be captured from a device that is not connected to a known (authenticated) Facebook user, which Meta can still acquire, then compared to stored voiceprints to identify the people so that Meta can push customized content to both people:

> [T]he social-networking system may use a process similar to that described above when the client device that detects speaking users is not authenticated to any of the speakers (for example, a

[13] *Id.* at 33-34 (diagram numbers omitted).

[14] *Id.* at 32 (diagram numbers omitted).

> BLUETOOTH beacon in a public place). As an example, suppose that Velma and Daphne walk into a store. Velma is known to be at the store (e.g., she opens a mobile application from the store on her smartphone). A beacon at the store may then detect Daphne speaking, and the social-networking system may identify Daphne based on a voiceprint analysis of Daphne's voice and based on Velma and Daphne being socially connected. This identification may occur even if the social-networking system does not otherwise detect Daphne's presence in the store (e.g., because location services, GPS, or the like are disabled or nonfunctional on her phone). The social-networking system may then send content or advertisements (e.g., a 2-for-1 coupon to the store; or an ad for a nearby store that may have relevance to both users) to Velma's and/or Daphne's device. Thus, in Daphne's case, content customized for Daphne's location may be sent to her despite her location services or GPS being disabled or non-functional.[15]

63. The 2020 Voiceprint Patent provided an example of another scenario by which Meta can more easily identify users with their voiceprints by limiting the pool of users for the voiceprint comparison based on an event:

> [I]dentification of users may also be applied to an event, in which case the event may correspond to a seed concept. For example, suppose that a restaurant invites people to an event, and 100 users confirm their attendance through the social-networking system. The restaurant has a BLUETOOTH beacon, and users may be identified by comparing their captured voices to stored voiceprints for the 100 attendees (as well as friends of the 100 attendees). In this way, the social-networking system need not compare captured voices to the voiceprints of social-network users who are not attendees at the event. Instead, the search space for the voiceprint comparison may be reduced from a large number of users of the social-networking system to the relatively small number of users who are associated with the event, such as the users who have confirmed their attendance on the social-networking system, and optionally their friends. Once attendees are identified, the social-networking system may present information to them that is tailored to their interests.[16]

64. The 2020 Voiceprint Patent provided an example of how users can be identified even when the audio is obtained by a device with no authenticated users connected to it:

[15] *Id.* at 32-33 (diagram numbers omitted).

[16] *Id.* at 33 (diagram numbers omitted).

> While the processes described above may involve a seed user or a seed concept, it is possible that initially there are no authenticated users. For example, suppose a user walks into a store and the location services or GPS on the user's client device are not active (e.g., BLUETOOTH is turned off and the client device does not have a good GPS signal). The BLUETOOTH beacon in the store receives the user's voice and the social-networking system identifies the user based on a comparison to voiceprints in the system. The system may compare the user's voice with many voiceprints to find a match. Alternatively, the system may apply filtering criteria based on time or location, e.g., to only consider voiceprints of users who have a recent location within a particular distance of the BLUETOOTH beacon.[17]

65. Accordingly, the 2020 Voiceprint Patent protected, *inter alia*, a method of, and software and processors for, using audio input of an unknown Facebook user (received by a known Facebook user) to identify the unknown Facebook user by comparing the audio input to the user's stored voiceprint:

> What is claimed is:
>
> 1. A method comprising, by one or more computing devices of an online social network:
>
> receiving, from a client system of a first user of the online social network, a first audio input from an unknown user;
>
> identifying one or more candidate users, wherein each candidate user is a user of the online social network within a threshold degree of separation of a known user;
>
> determining, for each candidate user, a proximity of the candidate user to the known user;
>
> calculating, for each candidate user, a probability score representing a probability that the unknown user is the candidate user, wherein the probability score is based on the proximity of the candidate user and a ***comparison of the first audio input to a voiceprint of the candidate user stored by the online social network, wherein each voiceprint comprises audio data for auditory identification of the candidate user***; and

[17] *Id.* (diagram numbers omitted).

> identifying one of the candidate users as being the unknown user based on the calculated probability scores of the candidate users.
>
> * * * *
>
> 14. One or more computer-readable non-transitory storage media embodying software that is operable when executed to:
>
> receive, from a client system of a first user of an online social network, a first audio input from an unknown user;
>
> identify one or more candidate users, wherein each candidate user is a user of the online social network within a threshold degree of separation of the first a known user;
>
> determine, for each candidate user, a proximity of the candidate user to the known user;
>
> calculate, for each candidate user, a probability score representing a probability that the unknown user is the candidate user, wherein the probability score is based on the proximity of the candidate user and a comparison of the first audio input to a voiceprint of the candidate user stored by the online social network, wherein each voiceprint comprises audio data for auditory identification of the candidate user; and
>
> identify one of the candidate users as being the unknown user based on the calculated probability scores of the candidate users.[18]

66. The 2020 Voiceprint Patent also protected a method of generating and storing a new voiceprint for the unknown user based on other identifying information received:

> What is claimed is:
>
> * * * *
>
> 11. The method of claim 1, further comprising:
>
> receiving identifying information for the unknown user;

[18] *Id.* at 51-52 (emphasis added). *See also id.* at ¶ 17 (claiming processors to perform the functions described above, including the "comparison of the first audio input to a voiceprint of the candidate user stored by the online social network").

> generating a new voiceprint based on the first audio input; and
>
> storing the new voiceprint in association with the identity information for subsequent access by the online social network.[19]

67. On January 10, 2020, Meta filed a patent application that incorporated, and was a continuation of the 2020 Voiceprint Patent.

68. The patent was issued on October 18, 2022, Patent No. 11,475,344 (the "2022 Voiceprint Patent").

69. The 2022 Voiceprint Patent was substantially similar to the 2020 Voiceprint Patent, but made additional claims related to Meta's method, software, and processors to, *inter alia*, use a voiceprint to identify a second user and authenticate access to an account.[20]

70. On August 26, 2022, Meta filed a patent application that incorporated, and was a continuation of the 2020 Voiceprint Patent and the 2022 Voiceprint Patent.

71. The patent was issued on May 2, 2023 (the "May 2023 Voiceprint Patent").

72. The May 2023 Voiceprint Patent was substantially similar to the 2020 Voiceprint Patent, but made additional claims related to Meta's method, software, and processors for determining what type of customizable content to deliver to a device of a first user based on audio of a second user received on the device of the first user:

> What is claimed is:
>
> 1. A method comprising:
>
> receiving, from a client system of a first user, an audio input from a second user, wherein a first user profile corresponding to the first user comprises first interest information associated with the first user, wherein a second

[19] *Id*. at 52-53.

[20] 2022 Voiceprint Patent, pp. 51-52.

> user profile corresponding to the second user comprises second interest information associated with the second user;
>
> determining, based on a comparison of the audio input to a voiceprint of the second user, wherein the voiceprint comprises audio data for auditory identification of the second user, whether the audio input comprises a query related to the first interest information and the second interest information; and
>
> sending, to the client system, customized content for presentation to the second user, wherein the content is customized using the first interest information and the second interest information.[21]

73. On July 13, 2023, Meta filed a patent application that incorporated, and was a continuation of the 2020 Voiceprint Patent, the 2022 Voiceprint Patent, and the May 2023 Voiceprint Patent (the "July 2023 Voiceprint Patent Application").

74. The July 2023 Voiceprint Patent Application was substantially similar to the prior Voiceprint Patents, but made additional claims related to Meta's method, software, and processors for identifying a second user from audio received from a *location*, rather than from a known first user, and sending customized content using Facebook interest information associated with the first or second user:

> What is claimed is:
>
> 1. A method comprising:
>
> receiving, from a client system at a first location, an audio input from an unknown user;
>
> identifying a first user who is proximate to the first location;
>
> identifying the unknown user as a second user based on a comparison of the audio input to one or more voiceprints of one or more candidate users accessible by the client system, respectively, wherein each voiceprint comprises audio data

[21] May 2023 Voiceprint Patent, p. 51-52. *See also id.* at 52-54 (claiming software and processors to carry out this method).

> for auditory identification of a unique user, and wherein each candidate user is a contact of the first user; and
>
> sending customized content to one or more of the first user or the second user, wherein the content is customized using interest information associated with the first or second user.
>
> * * * *
>
> 3. The method of claim 1, further comprising generating the customized content based on one or more interests of the first user or the second user, wherein the one or more interests are accessed from an online social network.
>
> 4. The method of claim 3, wherein the customized content comprises content having one or more topics that match the interests of the first user or the second user.
>
> 5. The method of claim 1, wherein the customized content comprises advertisements, news feeds, push notifications, place tips, coupons, suggestions, or a combination thereof.
>
> 6. The method of claim 1, wherein the client system is a mobile phone, a Bluetooth beacon, or a media device operable to receive audio input.[22]

IV. Meta Possesses, Creates, Collects, Captures, Receives Through Trade, and/or Otherwise Obtains Biometric Identifiers and Biometric Information

75. Numerous features of Meta allow it to collect audio of users' voices. For example, Meta's Messenger, which allows parties to send messages to one another, allows a user to utilize voice to text dictation, create and send voice messages, record/send videos with sound, and make voice and video calls. Facebook likewise allows users to, *inter alia*, search Facebook using a voice search and record and/or upload audio or videos with audio.

76. Meta receives the audio input from users when they utilize an audio function on Facebook or Messenger, including when they, *inter alia*, dictate a text message to send via

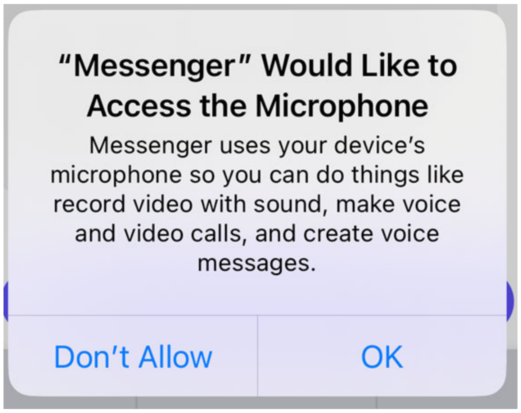
[22] July 2023 Voiceprint Patent Application, p. 27-28 *See also id.* at 28 (claiming software and processors to carry out the method of claim 1).

Messenger, send an audio recording via Messenger, make calls via Messenger, or provide audio data on Facebook, such as dictating a Facebook search, inputting their name pronunciation, posting an audio file, or posting a video that includes audio.

77. Upon information and belief, Meta also receives audio input of users from third party sources.

78. The audio input received by Meta can contain the voice of the person using the function or the voice of a person in the background.

79. Sometimes, a microphone is required to record audio or conduct a voice search. If the microphone function on a cell phone is turned off when a user seeks to utilize one of these audio functions on Messenger, Meta asks to "access the microphone," with a pop up that states: "'Messenger' Would Like to Access the Microphone. Messenger uses your device's microphone so you can do things like record video with sound, make voice and video calls, and create voice messages."



"Messenger" Would Like to Access the Microphone

Messenger uses your device's microphone so you can do things like record video with sound, make voice and video calls, and create voice messages.

80. The pop-up does not refer to any privacy policy, mention biometric data, or seek consent related to biometric data.

81. At least in 2023, and upon information and belief, for many years prior, Meta has been capturing, creating, collecting, and storing voiceprints and other biometric information of Facebook and Messenger users from audio data received via Facebook or Messenger and/or received from third parties.

82. Upon information and belief, Meta not only captures, creates, collects, and stores voiceprints and related biometric information of users who themselves speak or upload audio via Facebook or Messenger; it also captures, creates, collects, and stores voiceprints and related biometric information of users whose voices are included in audio uploaded by others via Facebook or Messenger.

83. From the audio input into Facebook or Messenger or otherwise received by Meta, Meta creates, captures, collects, stores, and/or obtains encoded digital data of the acoustic signals of the speaker's voice ("Digital Voice Data").

84. Meta processes the Digital Voice Data with, *inter alia*, an acoustical model, which is a model of the relationship between the audio signals and the sounds of phonetic units in the language.

85. The acoustical model is trained, and further refined, using the voice of a particular user, such that the acoustical model can be used to recognize that user by voice.

86. The acoustical model is further trained using the voices of many users to produce a speaker-independent model capable of recognizing multiple users by their voice.

87. Upon information and belief, Meta utilizes methods such as neural networks and deep learning models trained to extract distinctive characteristics of voices from the Digital Voice Data, such as the frequency pattern, frequency range, intonation, pitch, and accent, which output additional data based on the Digital Voice Data that can be and are used to identify an individual (the "Voice Characteristics").

88. Meta thus creates, captures, collects, stores, and/or obtains these Voice Characteristics.

89. Upon information and belief, Meta further creates and stores "Voice Profiles" for individual users, which store data specific to each individual user for use in subsequently recognizing each user by voice.

90. The Digital Voice Data that Meta creates, captures, stores, and/or obtains is a dataset, unique to an individual, that, combined with other data and tools at Meta's disposal, is capable of identifying that individual.

91. Moreover, the Digital Voice Data that Meta creates, captures, collects, stores, and/or obtains is actually used by Meta to identify people.

92. Meta's most recent privacy policy acknowledges that the Digital Voice Data, which it calls voice recordings, can be used to identify a person. *See* Meta United States Regional Privacy Notice[23] (Meta may collect "voice recordings which may be used to identify you . . . .").

93. Accordingly, the Digital Voice Data created, captured, collected, stored, and/or obtained by Meta constitutes a voiceprint, and thus, a "biometric identifier" under BIPA.

94. Alternatively, the Voice Characteristics, and/or Voice Profiles constitute voiceprints, and thus, a "biometric identifier" under BIPA.

95. Alternatively, the acoustical model, Voice Characteristics, and/or Voice Profiles are information based on a voiceprint used to identify an individual, and thus "biometric information" under BIPA.

96. Upon information and belief, Meta creates, captures, collects, stores, and/or obtains other data that is based on a voiceprint and used to identify an individual, which additional data constitutes "biometric information" under BIPA.

97. Upon information and belief, Meta uses the voiceprints and related biometric information in its possession to, *inter alia*, improve its voice recognition and identification

[23] https://www.facebook.com/privacy/policies/uso/ (last visited Aug. 8, 2023).

methods, software, processors, and machine learning; to improve its products and product development for hardware and software that utilize voice recognition, such as user authentication features; and to identify users so that it can send them customized, targeted content, including targeted advertisements.

V. Meta's Inadequate Disclosures Regarding Voiceprints

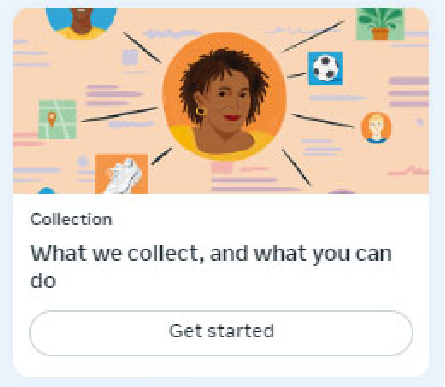
98. Meta's website purports to give users clear and easy access to information about data it collects, but its statements regarding privacy are contained on multiple webpages, popups, and supplemental terms, including in Meta's Privacy Center, an "Access Your Information" section within one's Facebook account, a Privacy Policy, and a United States Regional Privacy Policy.

99. Nowhere in these webpages, or anywhere else on its website, does Meta provide the disclosures or policies required by BIPA.

A. Meta's Privacy Center

100. Meta's website contains a "Privacy Center" describing in general terms the information it collects.

101. The Privacy Center contains a heading called "Collection," which states it covers "What we collect, and what you can do."[24]



Collection

What we collect, and what you can do

[24] Meta Privacy Center Home, https://www.facebook.com/privacy/center (last visited Aug. 10, 2023).

102. Clicking “Get Started” leads to a new webpage that states: “Collecting your information helps us create better experiences on our products, so you can discover more of what you love. But we know many people want options to manage the information we’ve collected, so let’s talk about the control you have.”[25]

103. The webpage has links with menus that open popup windows for more information, shown in the screenshot below. One heading invites the user to “Learn about information we collect.” Another states: “Are Facebook and Instagram listening to your conversations?” The next states: “How can you delete your information.” There is also a button to “Review your information.” Other links reference the Privacy Policy, suggesting that is where users can find out “What information do we collect?” and “How you can manage or delete your information.” Other links state: “Learn how we use your information” and “You have options to manage the ads you see on Facebook.”

///

///

///

///

///

///

///

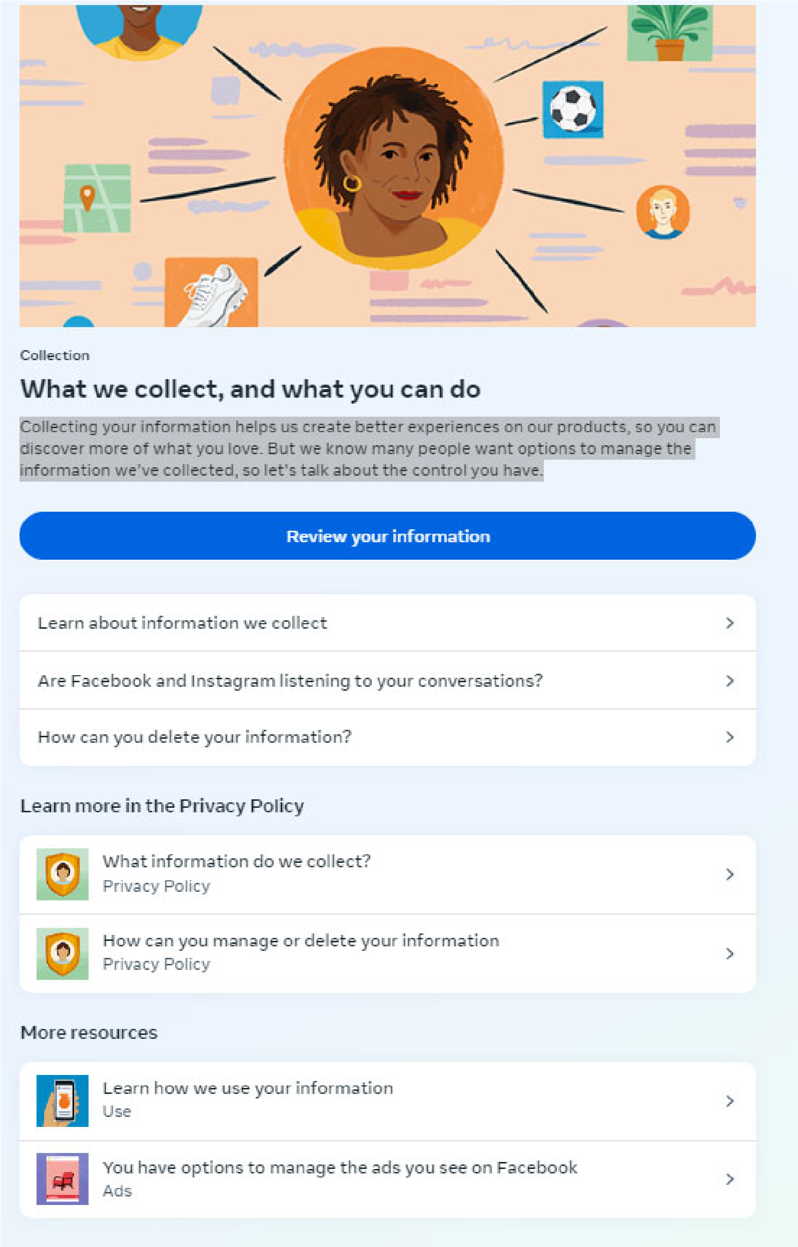
///

///

///

///

[25] https://www.facebook.com/privacy/guide/collection (last visited Aug. 10, 2023).



Collection

What we collect, and what you can do

Collecting your information helps us create better experiences on our products, so you can discover more of what you love. But we know many people want options to manage the information we've collected, so let's talk about the control you have.

Learn about information we collect ›

Are Facebook and Instagram listening to your conversations? ›

How can you delete your information? ›

Learn more in the Privacy Policy

What information do we collect?
Privacy Policy ›

How can you manage or delete your information
Privacy Policy ›

More resources

Learn how we use your information
Use ›

You have options to manage the ads you see on Facebook
Ads ›

///

///

///

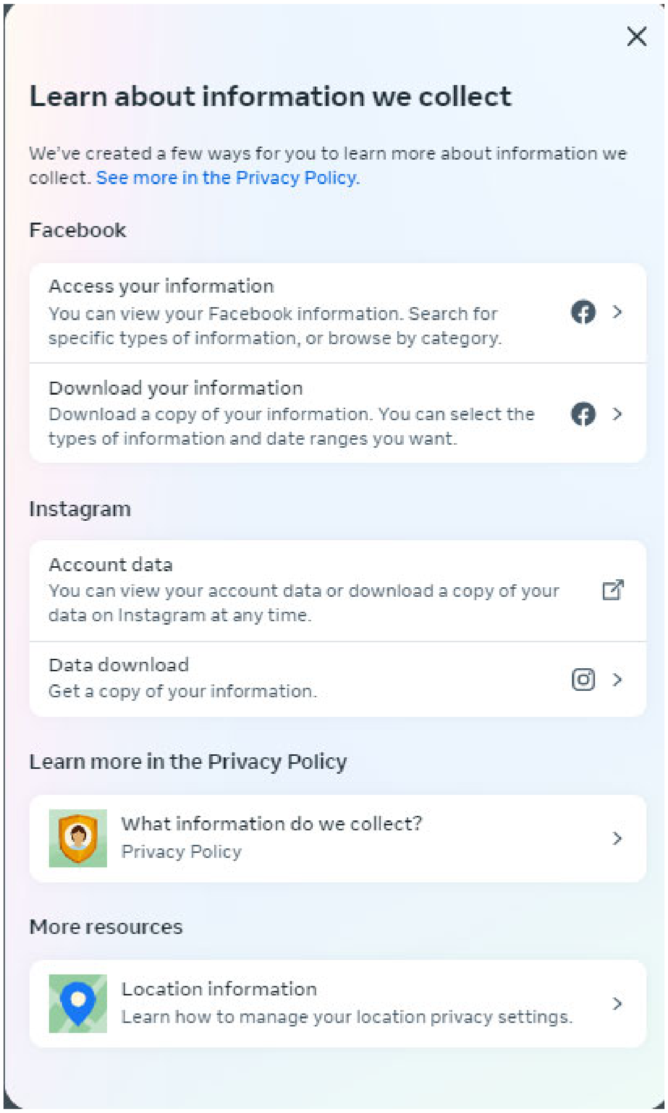
///

///

///

104. The link to "Review your information" leads to a Facebook login page. The user may log in to his or her Facebook account to obtain data Facebook provides about the user. As discussed in Section V.B below, nothing within those webpages discloses the existence of voiceprints or biometric information related thereto.

105. Clicking on "Learn about information we collect" opens a popup shown below[26] which provides another link to the Privacy Policy and links to access or download your information, both of which lead to the Facebook login page and process described above.



Learn about information we collect

We've created a few ways for you to learn more about information we collect. See more in the Privacy Policy.

Facebook

Access your information
You can view your Facebook information. Search for specific types of information, or browse by category.

Download your information
Download a copy of your information. You can select the types of information and date ranges you want.

Instagram

Account data
You can view your account data or download a copy of your data on Instagram at any time.

Data download
Get a copy of your information.

Learn more in the Privacy Policy

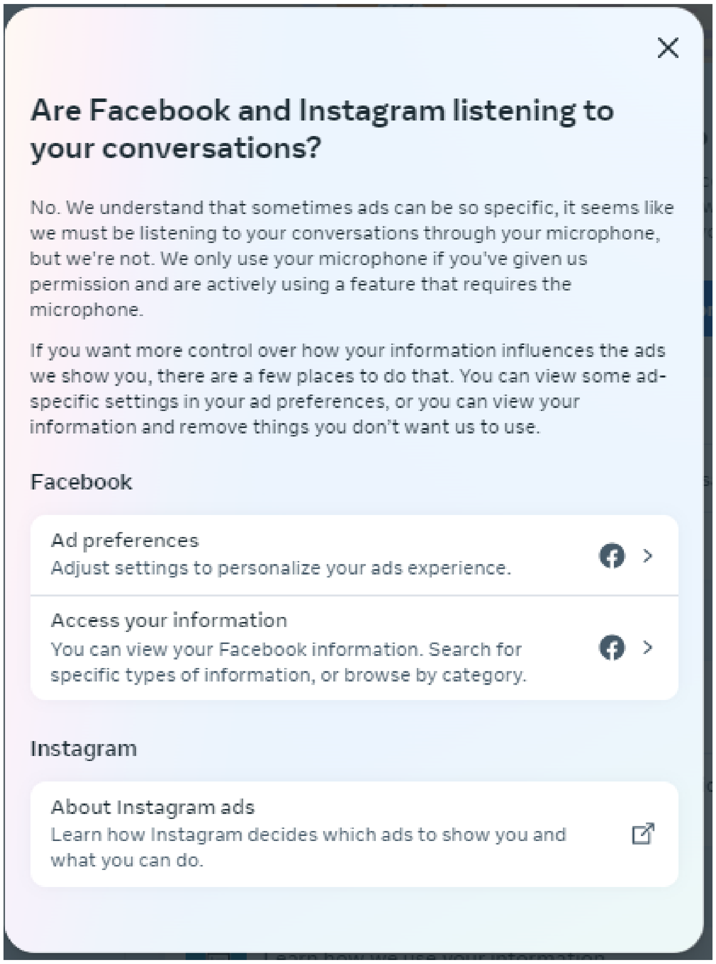
What information do we collect?
Privacy Policy

More resources

Location information
Learn how to manage your location privacy settings.

[26] *Available at* https://www.facebook.com/privacy/dialog/what-we-collect (last visited Aug. 10, 2023).

106. Returning to the "Collection" page and clicking "Are Facebook and Instagram listening to your conversations?" opens another popup shown below.[27] Meta states it is not listening to your conversations through your microphone, but states it uses your microphone with permission for certain audio features that require a microphone. There is no mention of what data is obtained when a user uses the microphone for one of those features.



Are Facebook and Instagram listening to your conversations?

No. We understand that sometimes ads can be so specific, it seems like we must be listening to your conversations through your microphone, but we're not. We only use your microphone if you've given us permission and are actively using a feature that requires the microphone.

If you want more control over how your information influences the ads we show you, there are a few places to do that. You can view some ad-specific settings in your ad preferences, or you can view your information and remove things you don't want us to use.

Facebook

Ad preferences
Adjust settings to personalize your ads experience.

Access your information
You can view your Facebook information. Search for specific types of information, or browse by category.

Instagram

About Instagram ads
Learn how Instagram decides which ads to show you and what you can do.

///

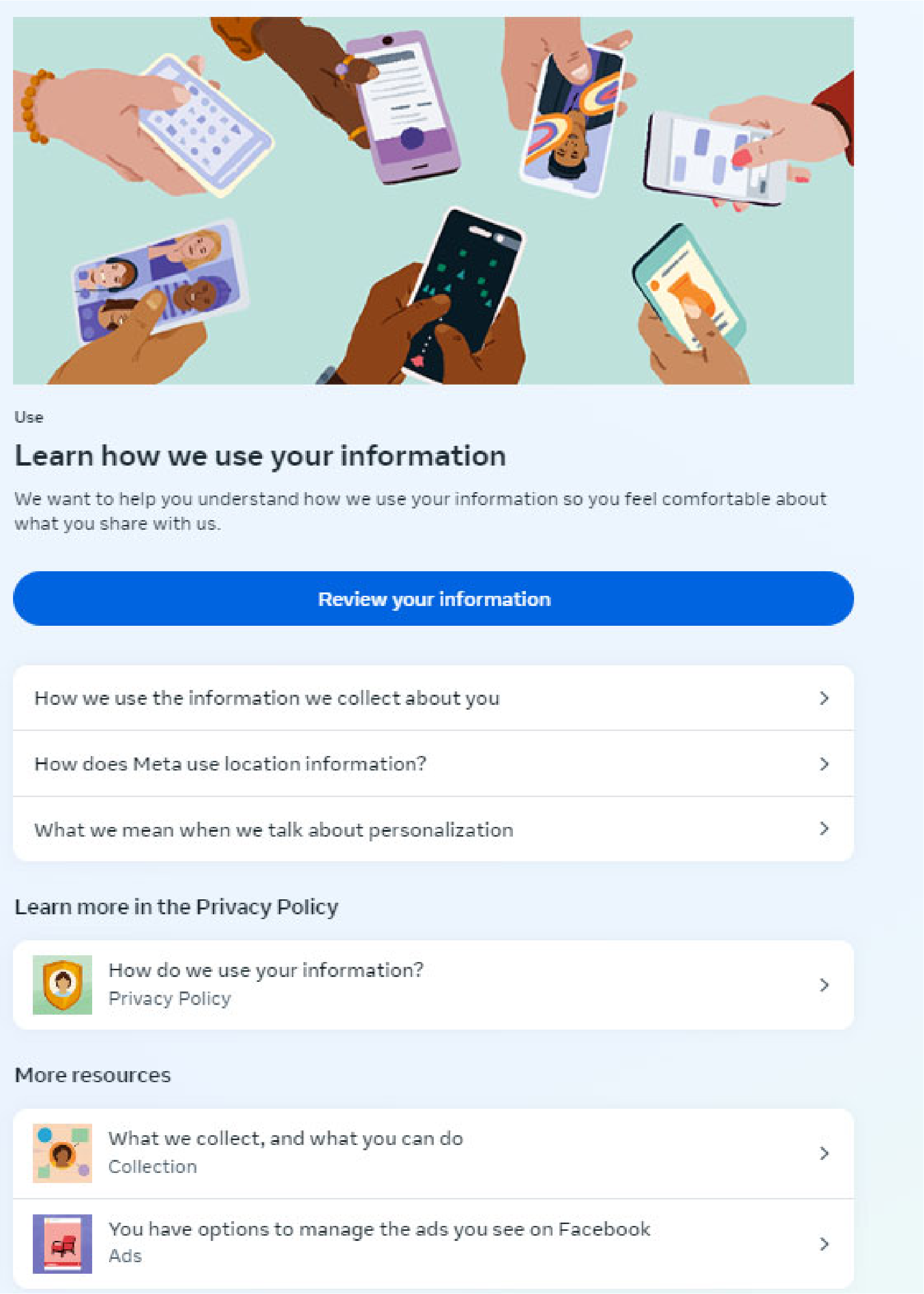
///

///

///

[27] *Available at* https://www.facebook.com/privacy/dialog/is-facebook-listening-to-my-conversation (last visited Aug. 10, 2023).

107. Returning to the "Collection" page and clicking "Learn how we use your information" opens another webpage shown below.[28]



Use

Learn how we use your information

We want to help you understand how we use your information so you feel comfortable about what you share with us.

How we use the information we collect about you ›
How does Meta use location information? ›
What we mean when we talk about personalization ›

Learn more in the Privacy Policy

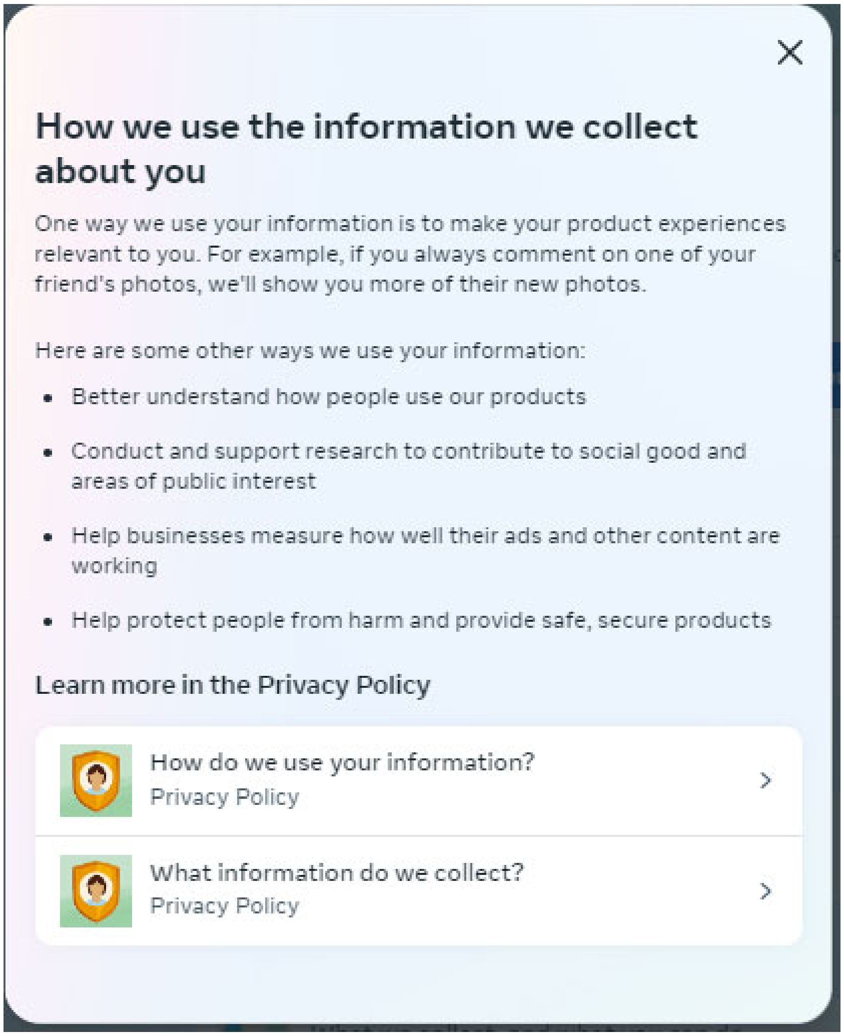
How do we use your information?
Privacy Policy ›

More resources

What we collect, and what you can do
Collection ›
You have options to manage the ads you see on Facebook
Ads ›

[28] https://www.facebook.com/privacy/guide/use/ (last visited Aug. 10, 2023).

108. Clicking on "How we use the information we collect about you" opens a popup shown below[29] that lists five ways Meta uses information it collects about users before directing them to the Privacy Policy:



How we use the information we collect about you

One way we use your information is to make your product experiences relevant to you. For example, if you always comment on one of your friend's photos, we'll show you more of their new photos.

Here are some other ways we use your information:

- Better understand how people use our products
- Conduct and support research to contribute to social good and areas of public interest
- Help businesses measure how well their ads and other content are working
- Help protect people from harm and provide safe, secure products

Learn more in the Privacy Policy

How do we use your information?
Privacy Policy

What information do we collect?
Privacy Policy

///

///

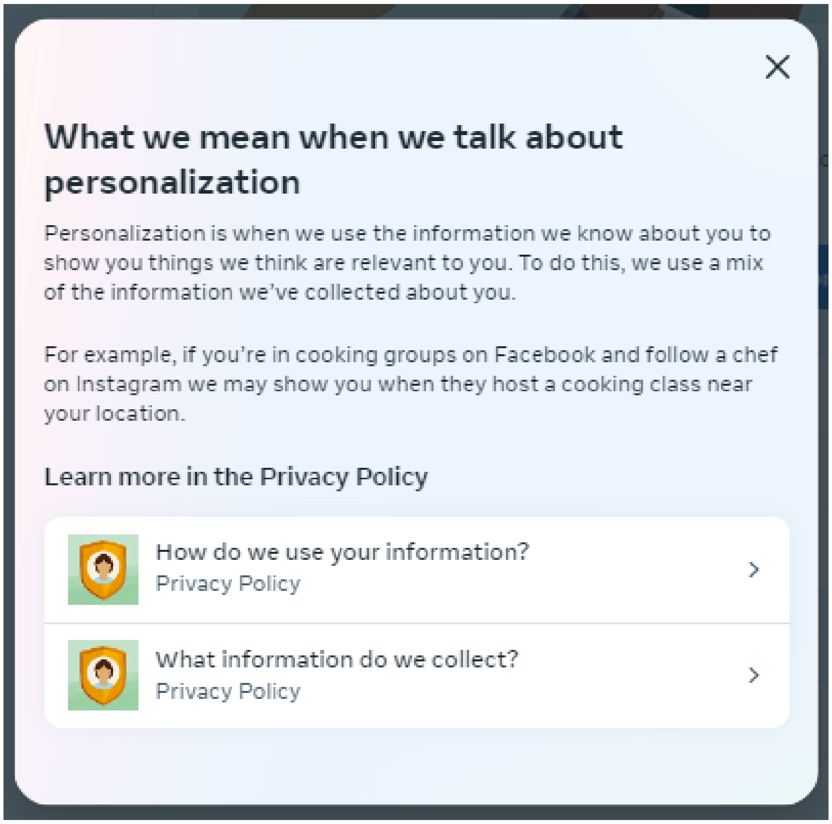
///

///

///

[29] *Available at* https://www.facebook.com/privacy/dialog/how-we-use-collected-information (last visited Aug. 10, 2023).

109. Returning to the "use" webpage and clicking "What we mean when we talk about personalization" opens a popup shown below[30] that directs users to the Privacy Policy and says, "[T]o show you things we think are relevant to you. . . . we use a mix of the information we've collected about you."



What we mean when we talk about personalization

Personalization is when we use the information we know about you to show you things we think are relevant to you. To do this, we use a mix of the information we've collected about you.

For example, if you're in cooking groups on Facebook and follow a chef on Instagram we may show you when they host a cooking class near your location.

Learn more in the Privacy Policy

How do we use your information?
Privacy Policy

What information do we collect?
Privacy Policy

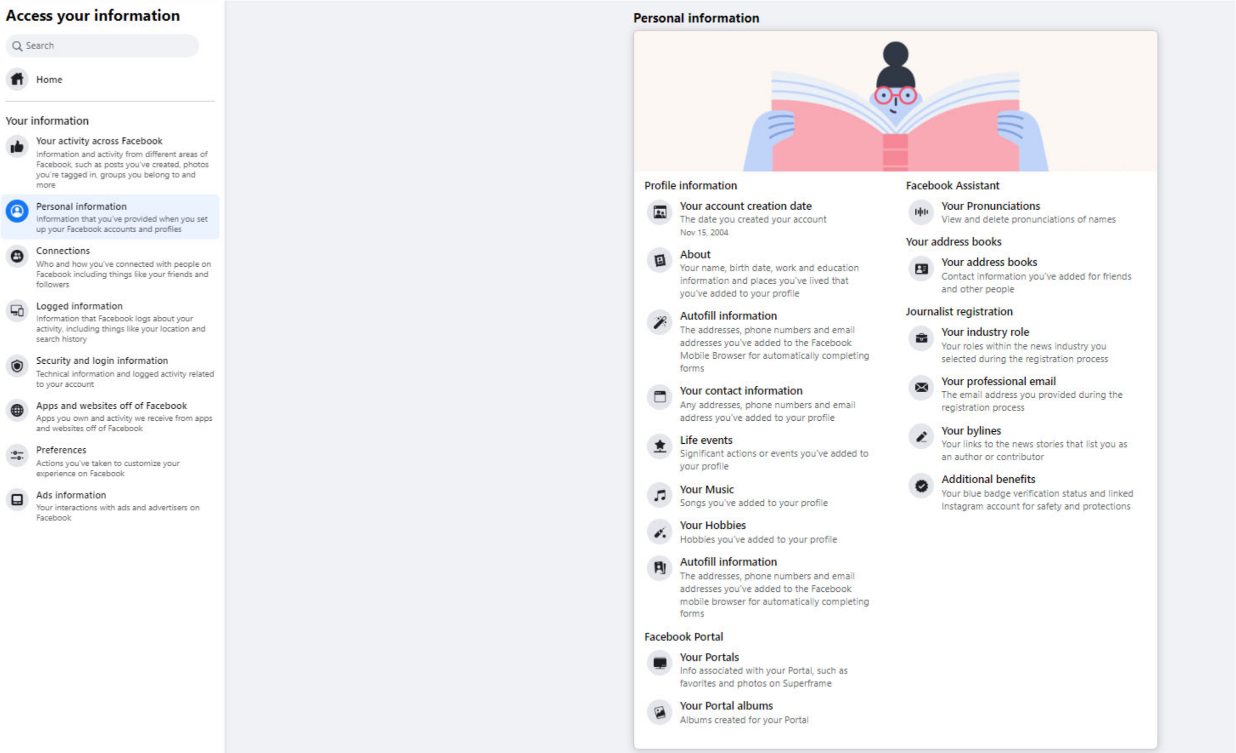
110. In short, nothing in this part of the Privacy Center discloses or describes the existence or use of voiceprints or biometric information related thereto.

B. Facebook's "Access Your Information"

111. Likewise, nothing in the section of Facebook where a user can review or download his or her own information discloses the existence or use of voiceprints or biometric information related thereto.

[30] *Available at* https://www.facebook.com/privacy/dialog/what-we-mean-when-we-talk-about-personalization (last visited Aug. 10, 2023).

112. This section of Facebook shows the logged-in user what information Meta is willing to provide the user, as shown in the screenshot below:



Access your information

Search

Home

Your information

Your activity across Facebook
Information and activity from different areas of Facebook, such as posts you've created, photos you're tagged in, groups you belong to and more

Personal information
Information that you've provided when you set up your Facebook accounts and profiles

Connections
Who and how you've connected with people on Facebook including things like your friends and followers

Logged information
Information that Facebook logs about your activity, including things like your location and search history

Security and login information
Technical information and logged activity related to your account

Apps and websites off of Facebook
Apps you own and activity we receive from apps and websites off of Facebook

Preferences
Actions you've taken to customize your experience on Facebook

Ads information
Your interactions with ads and advertisers on Facebook

Personal information

Profile information

Your account creation date
The date you created your account
Nov 15, 2004

About
Your name, birth date, work and education information and places you've lived that you've added to your profile

Autofill information
The addresses, phone numbers and email addresses you've added to the Facebook Mobile Browser for automatically completing forms

Your contact information
Any addresses, phone numbers and email address you've added to your profile

Life events
Significant actions or events you've added to your profile

Your Music
Songs you've added to your profile

Your Hobbies
Hobbies you've added to your profile

Autofill information
The addresses, phone numbers and email addresses you've added to the Facebook mobile browser for automatically completing forms

Facebook Portal

Your Portals
Info associated with your Portal, such as favorites and photos on Superframe

Your Portal albums
Albums created for your Portal

Facebook Assistant

Your Pronunciations
View and delete pronunciations of names

Your address books

Your address books
Contact information you've added for friends and other people

Journalist registration

Your industry role
Your roles within the news industry you selected during the registration process

Your professional email
The email address you provided during the registration process

Your bylines
Your links to the news stories that list you as an author or contributor

Additional benefits
Your blue badge verification status and linked Instagram account for safety and protections

///

///

///

///

///

///

///

///

///

///

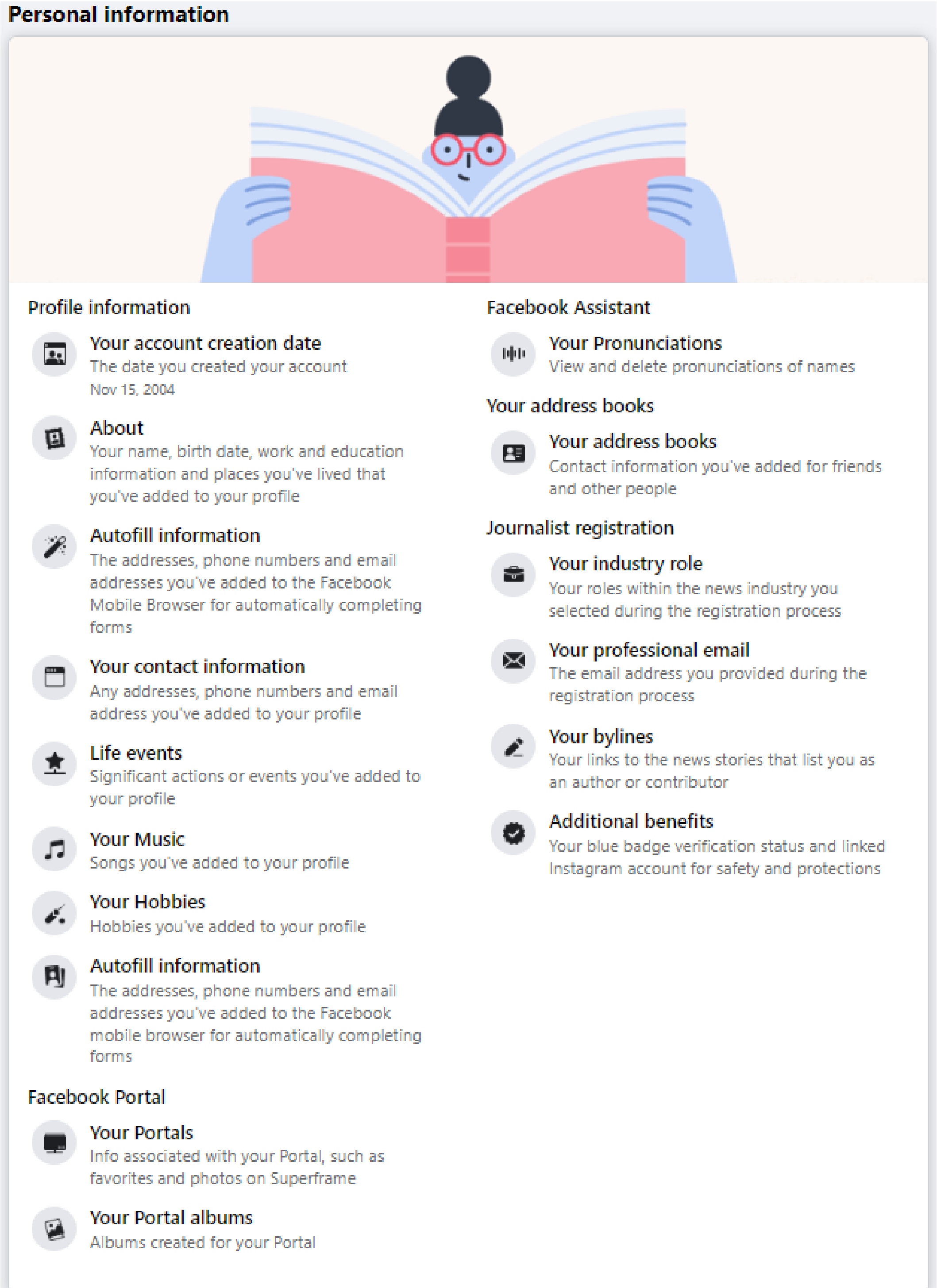
///

///

///

///

113. Nothing in the "Personal Information" section indicates that Meta collects voiceprints or other related biometric information. Below is a zoomed-in screenshot of the image above:



Personal information

Profile information

Your account creation date
The date you created your account
Nov 15, 2004

About
Your name, birth date, work and education information and places you've lived that you've added to your profile

Autofill information
The addresses, phone numbers and email addresses you've added to the Facebook Mobile Browser for automatically completing forms

Your contact information
Any addresses, phone numbers and email address you've added to your profile

Life events
Significant actions or events you've added to your profile

Your Music
Songs you've added to your profile

Your Hobbies
Hobbies you've added to your profile

Autofill information
The addresses, phone numbers and email addresses you've added to the Facebook mobile browser for automatically completing forms

Facebook Portal

Your Portals
Info associated with your Portal, such as favorites and photos on Superframe

Your Portal albums
Albums created for your Portal

Facebook Assistant

Your Pronunciations
View and delete pronunciations of names

Your address books

Your address books
Contact information you've added for friends and other people

Journalist registration

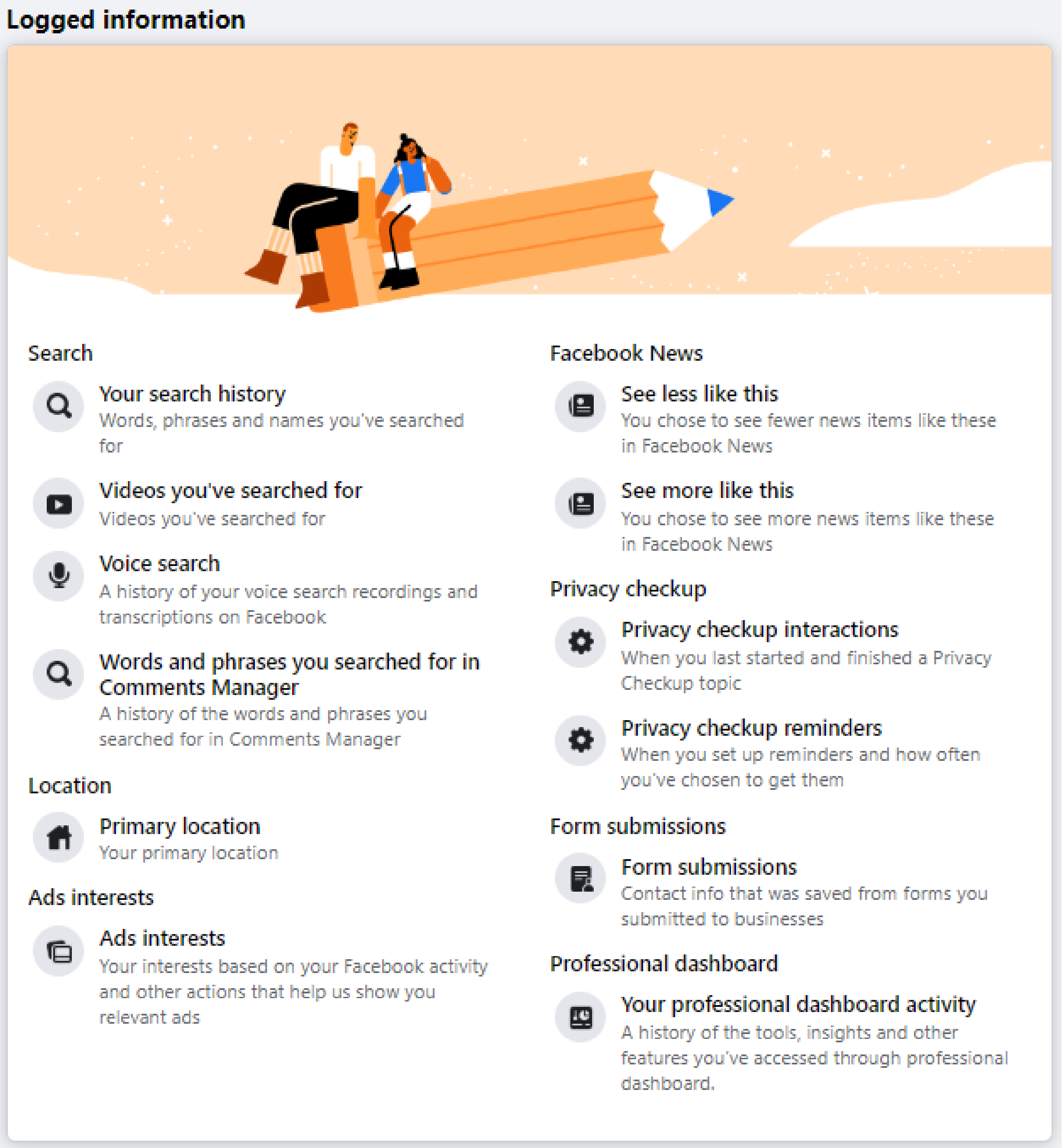
Your industry role
Your roles within the news industry you selected during the registration process

Your professional email
The email address you provided during the registration process

Your bylines
Your links to the news stories that list you as an author or contributor

Additional benefits
Your blue badge verification status and linked Instagram account for safety and protections

114. As shown in the screenshot below, when a user seeks to access his or her "Logged information," there is an indication that Meta has voice search recordings and transcriptions, but no indication that Meta collects voiceprints or other related biometric information.



Logged information

Search

- Your search history
  Words, phrases and names you've searched for
- Videos you've searched for
  Videos you've searched for
- Voice search
  A history of your voice search recordings and transcriptions on Facebook
- Words and phrases you searched for in Comments Manager
  A history of the words and phrases you searched for in Comments Manager

Location

- Primary location
  Your primary location

Ads interests

- Ads interests
  Your interests based on your Facebook activity and other actions that help us show you relevant ads

Facebook News

- See less like this
  You chose to see fewer news items like these in Facebook News
- See more like this
  You chose to see more news items like these in Facebook News

Privacy checkup

- Privacy checkup interactions
  When you last started and finished a Privacy Checkup topic
- Privacy checkup reminders
  When you set up reminders and how often you've chosen to get them

Form submissions

- Form submissions
  Contact info that was saved from forms you submitted to businesses

Professional dashboard

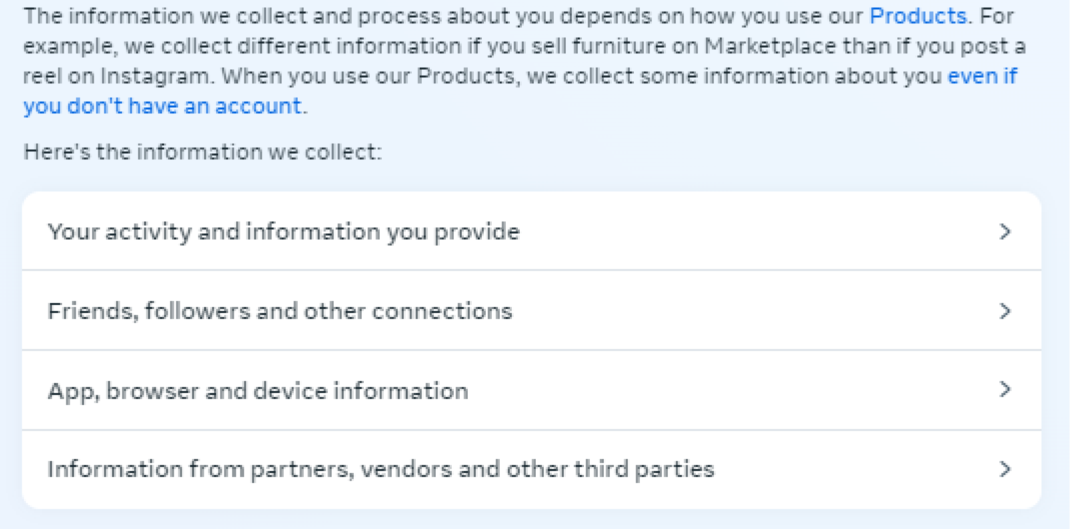
- Your professional dashboard activity
  A history of the tools, insights and other features you've accessed through professional dashboard.

115. No other section of the Access Your Information section of a user's Facebook profile mentions voiceprints or related biometric information.

C. Meta's Privacy Policy

116. Likewise, nothing in Meta's Privacy Policy discloses the existence or use of voiceprints or biometric information related thereto.

117. The Privacy Policy states: "The information we collect and process about you depends on how you use our Products. For example, we collect different information if you sell furniture on Marketplace than if you post a reel on Instagram. When you use our Products, we collect some information about you even if you don't have an account." It continues to describe "the information we collect" in categories of "Your activity and information you provide"; "Friends, followers and other connections"; "App, browser and device information"; and "Information from partners, vendors and other third parties."[31]



The information we collect and process about you depends on how you use our Products. For example, we collect different information if you sell furniture on Marketplace than if you post a reel on Instagram. When you use our Products, we collect some information about you even if you don't have an account.

Here's the information we collect:

Your activity and information you provide >
Friends, followers and other connections >
App, browser and device information >
Information from partners, vendors and other third parties >

///

///

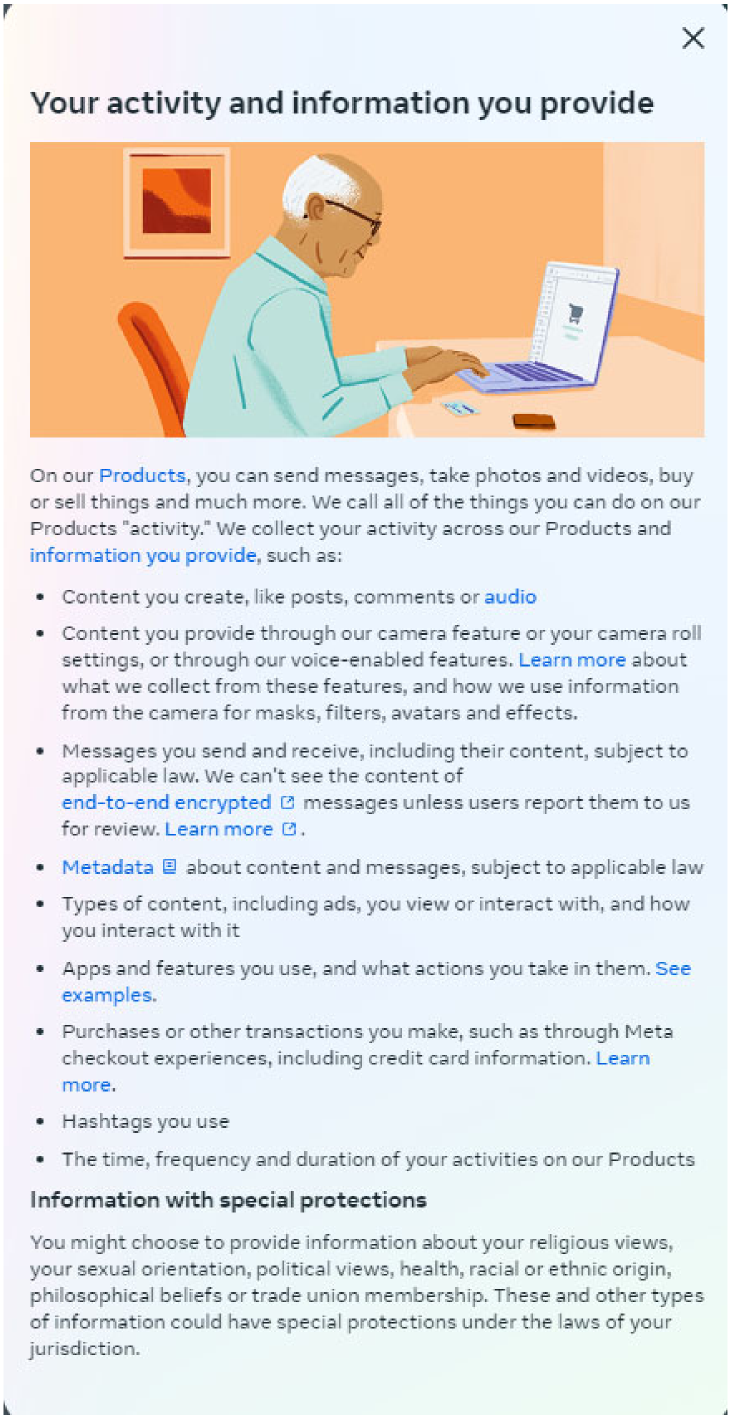
///

///

///

[31] Meta Privacy Policy, Effective June 15, 2023, https://ww.facebook.com/privacy/policy (last visited Aug. 8, 2023).

118. Clicking "Your activity and information you provide" opens a popup shown below,[32] which explains that "activity" means anything done on a Meta Product, and includes "[c]ontent you create, like posts, comments or audio."



Your activity and information you provide

On our Products, you can send messages, take photos and videos, buy or sell things and much more. We call all of the things you can do on our Products "activity." We collect your activity across our Products and information you provide, such as:

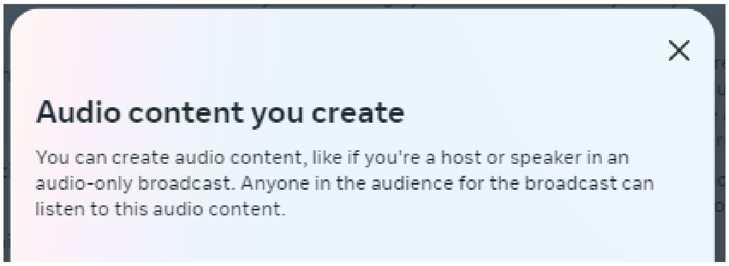
- Content you create, like posts, comments or audio
- Content you provide through our camera feature or your camera roll settings, or through our voice-enabled features. Learn more about what we collect from these features, and how we use information from the camera for masks, filters, avatars and effects.
- Messages you send and receive, including their content, subject to applicable law. We can't see the content of end-to-end encrypted messages unless users report them to us for review. Learn more.
- Metadata about content and messages, subject to applicable law
- Types of content, including ads, you view or interact with, and how you interact with it
- Apps and features you use, and what actions you take in them. See examples.
- Purchases or other transactions you make, such as through Meta checkout experiences, including credit card information. Learn more.
- Hashtags you use
- The time, frequency and duration of your activities on our Products

Information with special protections

You might choose to provide information about your religious views, your sexual orientation, political views, health, racial or ethnic origin, philosophical beliefs or trade union membership. These and other types of information could have special protections under the laws of your jurisdiction.

[32] *Available at* https://www.facebook.com/privacy/policy?subpage=1.subpage.1-YourActivityAndInformation (last visited Aug. 8, 2023).

119. Clicking on the link "audio" opens another popup shown below[33] that simply states a user "can create audio content."

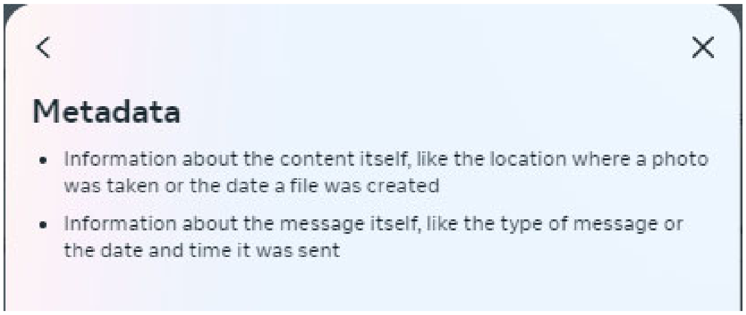


Audio content you create

You can create audio content, like if you're a host or speaker in an audio-only broadcast. Anyone in the audience for the broadcast can listen to this audio content.

120. Returning to the prior popup and clicking on the link to "Learn More" about "what we collect from" "our voice-enabled features" opens another popup[34] that provides an example of Meta collecting a voice interaction with Meta's voice-enabled assistant on its Ray-Ban Stories product. There is no mention of voiceprints or related biometric data, or of such information obtained from Facebook or Messenger.

121. Returning to the prior popup and clicking on the link to "Metadata" opens a new popup shown below[35] that generally states metadata is information about the content or message:



Metadata

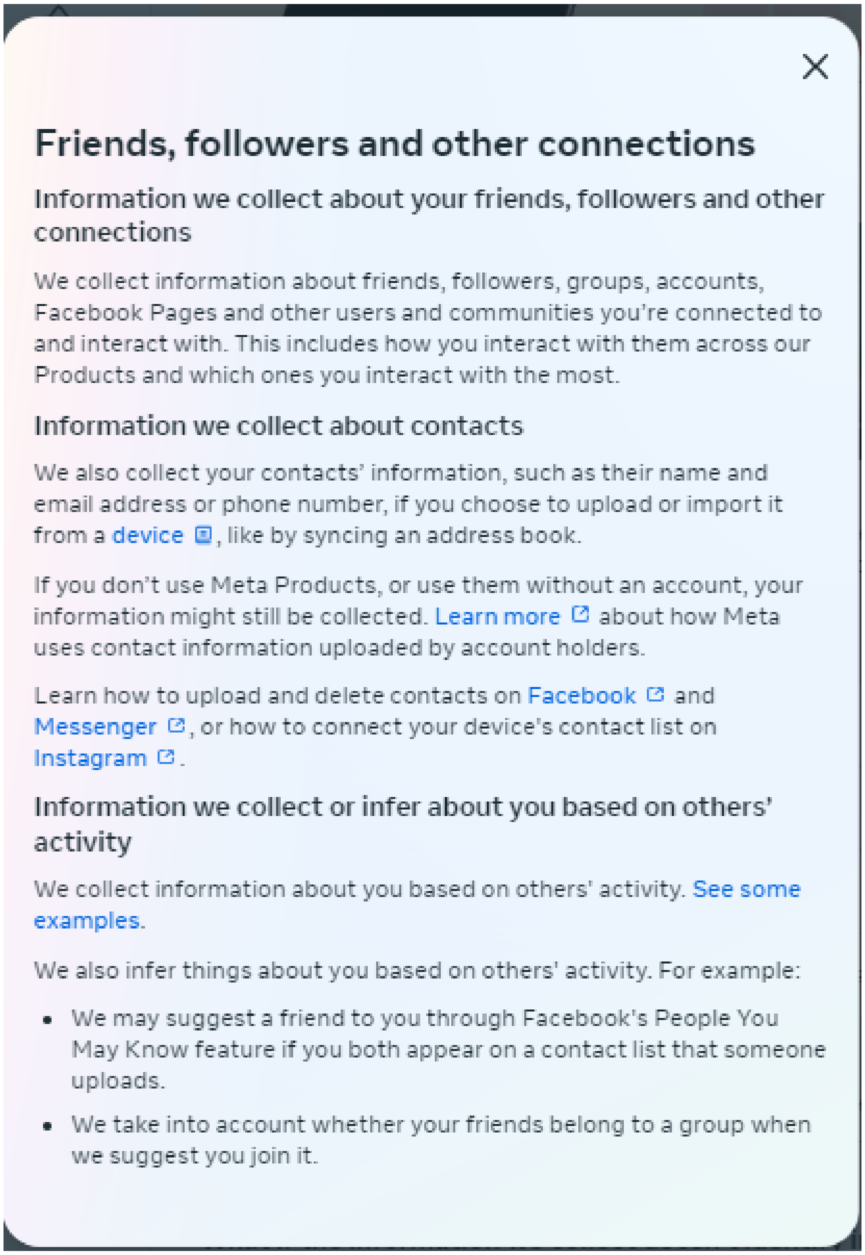
- Information about the content itself, like the location where a photo was taken or the date a file was created
- Information about the message itself, like the type of message or the date and time it was sent

[33] *Available at* https://www.facebook.com/privacy/policy?annotations[0]=1.ex.6-AudioContentYouCreate&subpage=1.subpage.1-YourActivityAndInformation (last visited Aug. 8, 2023).

[34] *Available at* https://www.facebook.com/privacy/policy?annotations[0]=1.story.3-WhatWeCollectFrom&subpage=1.subpage.1-YourActivityAndInformation (last visited Aug. 8, 2023).

[35] *Available at* https://www.facebook.com/privacy/policy?annotations[0]=Definition-Metadata&subpage=1.subpage.1-YourActivityAndInformation (last visited Aug. 8, 2023).

122. Returning to the Privacy Policy and clicking the link discussing information collected from friends and followers vaguely indicates, "We collect information about you based on others' activity," as shown in the screenshot below:[36]



Friends, followers and other connections

Information we collect about your friends, followers and other connections

We collect information about friends, followers, groups, accounts, Facebook Pages and other users and communities you're connected to and interact with. This includes how you interact with them across our Products and which ones you interact with the most.

Information we collect about contacts

We also collect your contacts' information, such as their name and email address or phone number, if you choose to upload or import it from a device, like by syncing an address book.

If you don't use Meta Products, or use them without an account, your information might still be collected. Learn more about how Meta uses contact information uploaded by account holders.

Learn how to upload and delete contacts on Facebook and Messenger, or how to connect your device's contact list on Instagram.

Information we collect or infer about you based on others' activity

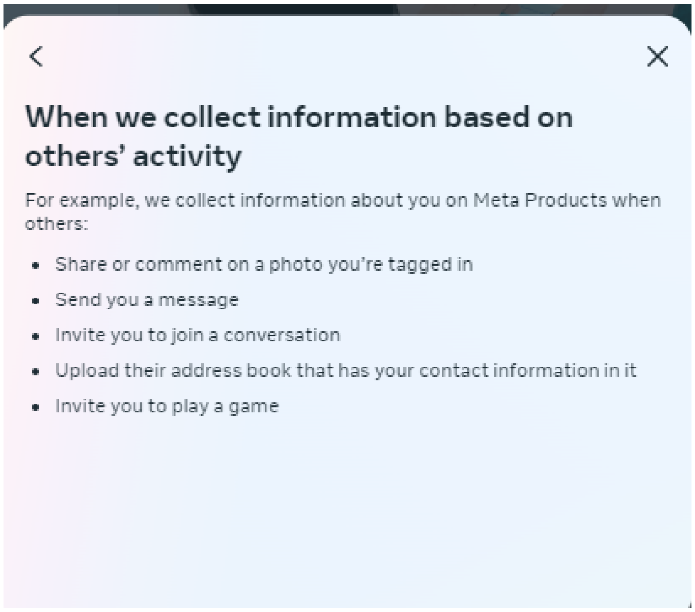
We collect information about you based on others' activity. See some examples.

We also infer things about you based on others' activity. For example:

- We may suggest a friend to you through Facebook's People You May Know feature if you both appear on a contact list that someone uploads.
- We take into account whether your friends belong to a group when we suggest you join it.

[36] *Available at* https://www.facebook.com/privacy/policy?subpage=1.subpage.2-FriendsFollowersAndOther (last visited Aug. 8, 2023).

123. Clicking on “See some examples” opens a popup shown below listing five examples, none of which indicate that audio of a user sent by another user may be used to create a voiceprint of the non-sending user or identify that user by comparing the audio to a voiceprint of the user.



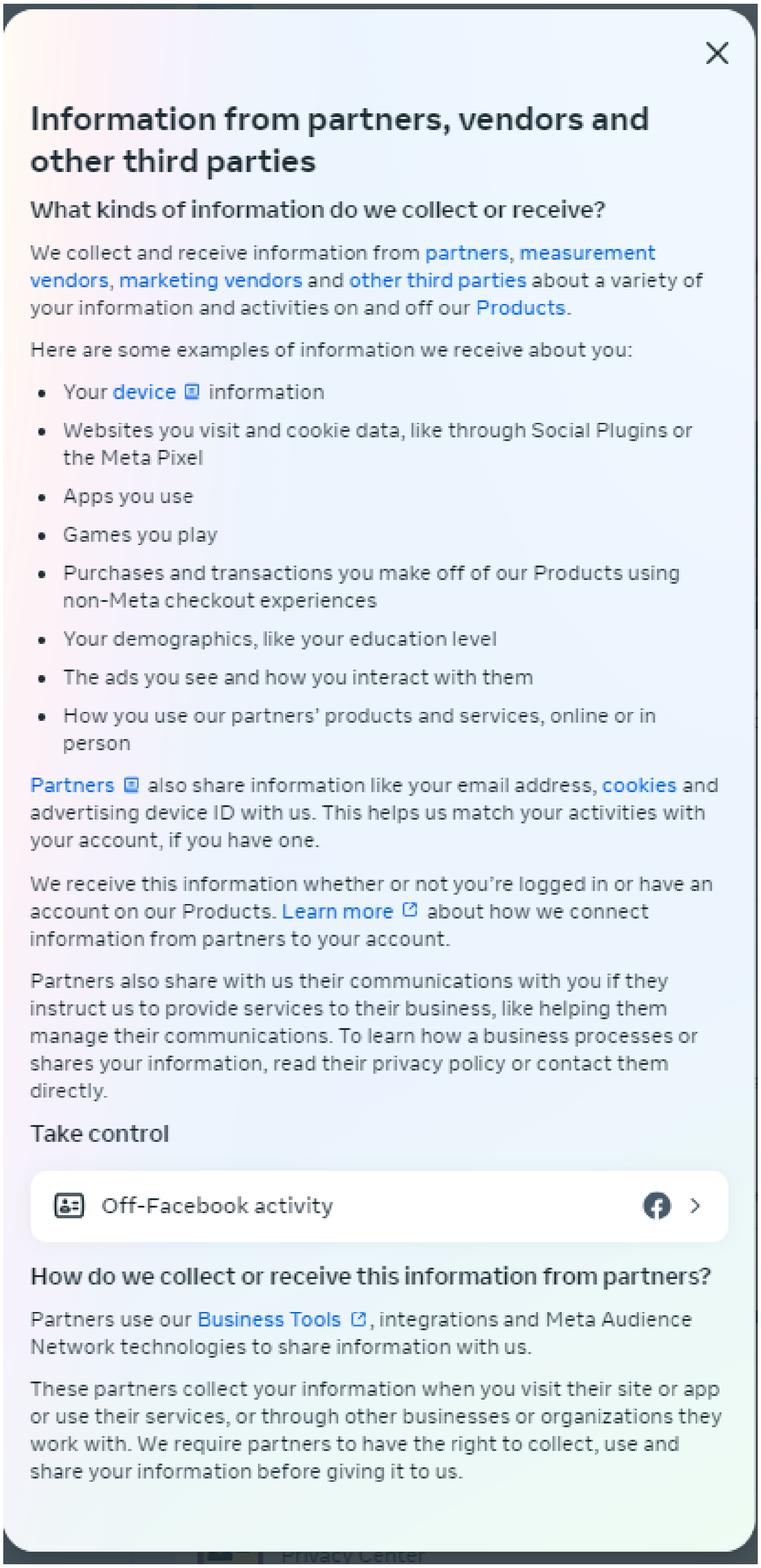
When we collect information based on others’ activity

For example, we collect information about you on Meta Products when others:

- Share or comment on a photo you’re tagged in
- Send you a message
- Invite you to join a conversation
- Upload their address book that has your contact information in it
- Invite you to play a game

124. Returning to the Privacy Policy and clicking the link discussing information collected from partners, vendors and other third parties opens a popup which states that Meta collects information from third parties “about a variety of your information and activities on and off our Products,” as shown in the screenshot below:[37]

[37] *Available at* https://www.facebook.com/privacy/policy?subpage=1.subpage.4-InformationFromPartnersVendors (last visited Aug. 8, 2023).



Information from partners, vendors and other third parties

What kinds of information do we collect or receive?

We collect and receive information from partners, measurement vendors, marketing vendors and other third parties about a variety of your information and activities on and off our Products.

Here are some examples of information we receive about you:

- Your device information
- Websites you visit and cookie data, like through Social Plugins or the Meta Pixel
- Apps you use
- Games you play
- Purchases and transactions you make off of our Products using non-Meta checkout experiences
- Your demographics, like your education level
- The ads you see and how you interact with them
- How you use our partners' products and services, online or in person

Partners also share information like your email address, cookies and advertising device ID with us. This helps us match your activities with your account, if you have one.

We receive this information whether or not you're logged in or have an account on our Products. Learn more about how we connect information from partners to your account.

Partners also share with us their communications with you if they instruct us to provide services to their business, like helping them manage their communications. To learn how a business processes or shares your information, read their privacy policy or contact them directly.

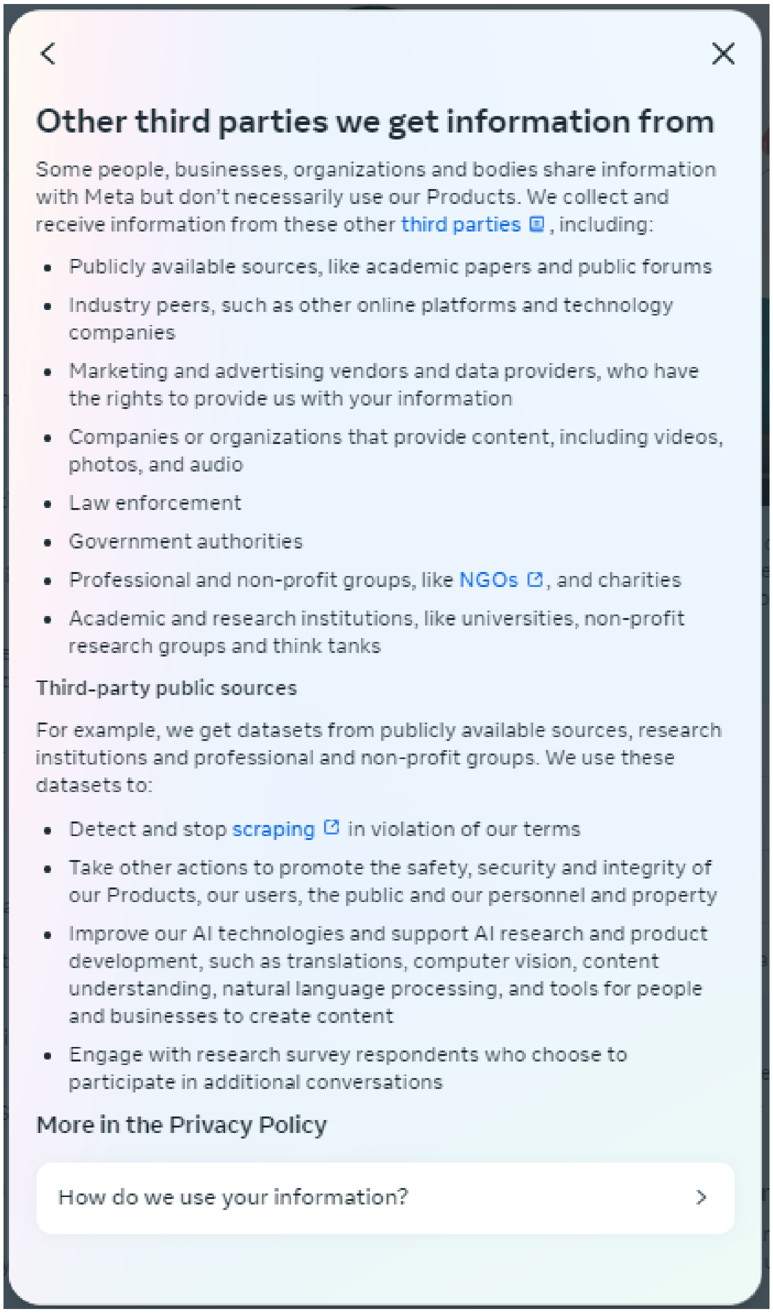
Take control

How do we collect or receive this information from partners?

Partners use our Business Tools, integrations and Meta Audience Network technologies to share information with us.

These partners collect your information when you visit their site or app or use their services, or through other businesses or organizations they work with. We require partners to have the right to collect, use and share your information before giving it to us.

125. Clicking on the "other third parties" link opens a new popup shown below[38] that indicates Meta receives audio from some companies or organizations that do not necessarily use Meta's Products.



Other third parties we get information from

Some people, businesses, organizations and bodies share information with Meta but don't necessarily use our Products. We collect and receive information from these other third parties, including:

- Publicly available sources, like academic papers and public forums
- Industry peers, such as other online platforms and technology companies
- Marketing and advertising vendors and data providers, who have the rights to provide us with your information
- Companies or organizations that provide content, including videos, photos, and audio
- Law enforcement
- Government authorities
- Professional and non-profit groups, like NGOs, and charities
- Academic and research institutions, like universities, non-profit research groups and think tanks

Third-party public sources

For example, we get datasets from publicly available sources, research institutions and professional and non-profit groups. We use these datasets to:

- Detect and stop scraping in violation of our terms
- Take other actions to promote the safety, security and integrity of our Products, our users, the public and our personnel and property
- Improve our AI technologies and support AI research and product development, such as translations, computer vision, content understanding, natural language processing, and tools for people and businesses to create content
- Engage with research survey respondents who choose to participate in additional conversations

More in the Privacy Policy

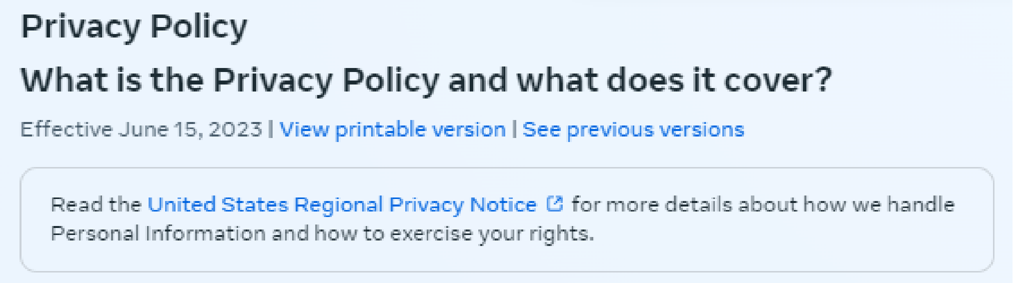
[38] *Available at* https://www.facebook.com/privacy/policy?annotations[0]=1.ex.40-ThirdPartiesWeGet&subpage=1.subpage.4-InformationFromPartnersVendors (last visited Aug. 8, 2023).

126. Nothing in the Privacy Policy indicates that audio of a user sent by a third party may be used to create a voiceprint of a Facebook user or identify that user by comparing it to a voiceprint.

127. In sum, the Privacy Policy does not disclose that Meta creates, captures, collects, obtains, and utilizes voiceprints or related biometric information.

D. Meta's United States Regional Privacy Notice

128. Near the top of the Privacy Policy is a sentence stating: "Read the United States Regional Privacy Notice for more details about how we handle Personal Information and how to exercise your rights."[39]



Privacy Policy

What is the Privacy Policy and what does it cover?

Effective June 15, 2023 | View printable version | See previous versions

Read the United States Regional Privacy Notice for more details about how we handle Personal Information and how to exercise your rights.

129. The Privacy Policy does not indicate that the United States Regional Privacy Notice is applicable to all U.S. residents or that it contains supplemental terms to the Privacy Policy.

130. Prior to January 1, 2023, clicking on the link lead to a "California Privacy Notice," which was applicable only to California residents.[40]

///

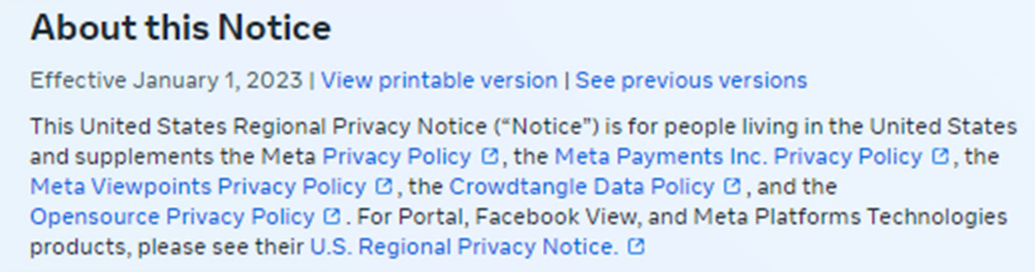
///

///

[39] Meta Privacy Policy, Effective June 15, 2023, https://ww.facebook.com/privacy/policy (last visited Aug. 8, 2023).

[40] *Available at* https://www.facebook.com/privacy/policies/uso/version/20220726/ (last visited Aug. 8, 2023).

131. As of January 1, 2023, clicking on the link in the Privacy Policy to "United States Regional Privacy Notice" (the "U.S. Privacy Notice") reveals additional terms that "supplement[]" Meta's Privacy Policy for all people living in the United States.[41]



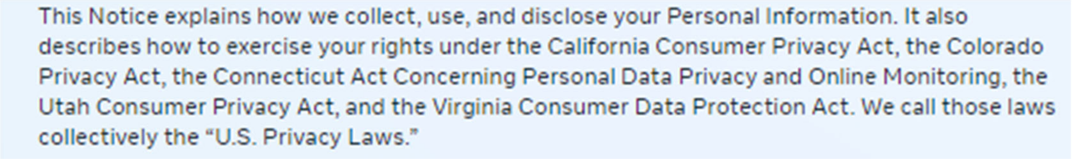
About this Notice

Effective January 1, 2023 | View printable version | See previous versions

This United States Regional Privacy Notice ("Notice") is for people living in the United States and supplements the Meta Privacy Policy ⧉, the Meta Payments Inc. Privacy Policy ⧉, the Meta Viewpoints Privacy Policy ⧉, the Crowdtangle Data Policy ⧉, and the Opensource Privacy Policy ⧉. For Portal, Facebook View, and Meta Platforms Technologies products, please see their U.S. Regional Privacy Notice. ⧉

132. The U.S. Privacy Notice as updated on July 1, 2023. The provisions described herein are contained in both the January 2023 and July 2023 versions.

133. The U.S. Privacy Notice purports to explain how Meta collects, uses, and discloses Personal Information and "describes how to exercise your rights under" California, Colorado, Connecticut, Utah, and Virginia privacy laws.[42] There is no mention of Illinois law.



This Notice explains how we collect, use, and disclose your Personal Information. It also describes how to exercise your rights under the California Consumer Privacy Act, the Colorado Privacy Act, the Connecticut Act Concerning Personal Data Privacy and Online Monitoring, the Utah Consumer Privacy Act, and the Virginia Consumer Data Protection Act. We call those laws collectively the "U.S. Privacy Laws."

134. The U.S. Privacy Notice explains that the term "Personal Information" means "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked with you, directly or indirectly."[43]

[41] U.S. Privacy Notice, Effective January 1, 2023, *available at* https://www.facebook.com/privacy/policies/uso/version/5555449491171442/ (last visited Aug. 8, 2023).

[42] U.S. Privacy Notice, Effective July 1, 2023, https://www.facebook.com/privacy/policies/uso/ (last visited Aug. 8, 2023).

[43] *Id.*

135. The U.S. Privacy Notice states that Meta "process[es] information about you, including Personal Information, whether or not you have an account or are logged in."[44]

136. The U.S. Privacy Notice states that Meta "may disclose your Personal Information for business purposes . . . ."[45]

137. The U.S. Privacy Notice provides a "summary" of "[t]he categories of Personal Information we may have collected about you over the past 12 months," "[h]ow we may use your Personal Information," and "[t]o whom we may have disclosed that information."[46]

138. The categories of Personal Information collected include, *inter alia*:

- Identifiers;
- Photos and videos, which may include face imagery;
- Internet or other electronic network activity information, including browser and app logs, content you view or engage with, and app, browser and device information;
- Location-related information; and
- Audio or visual information, including photos, videos, and voice recordings.[47]

139. The U.S. Privacy Notice continues, explaining that Meta may also collect additional "sensitive personal information" (as defined in the privacy laws of California, Colorado, Connecticut, Utah, and Virginia), including, *inter alia*:

[44] *Id.*

[45] *Id.*

[46] *Id.*

[47] *Id.*

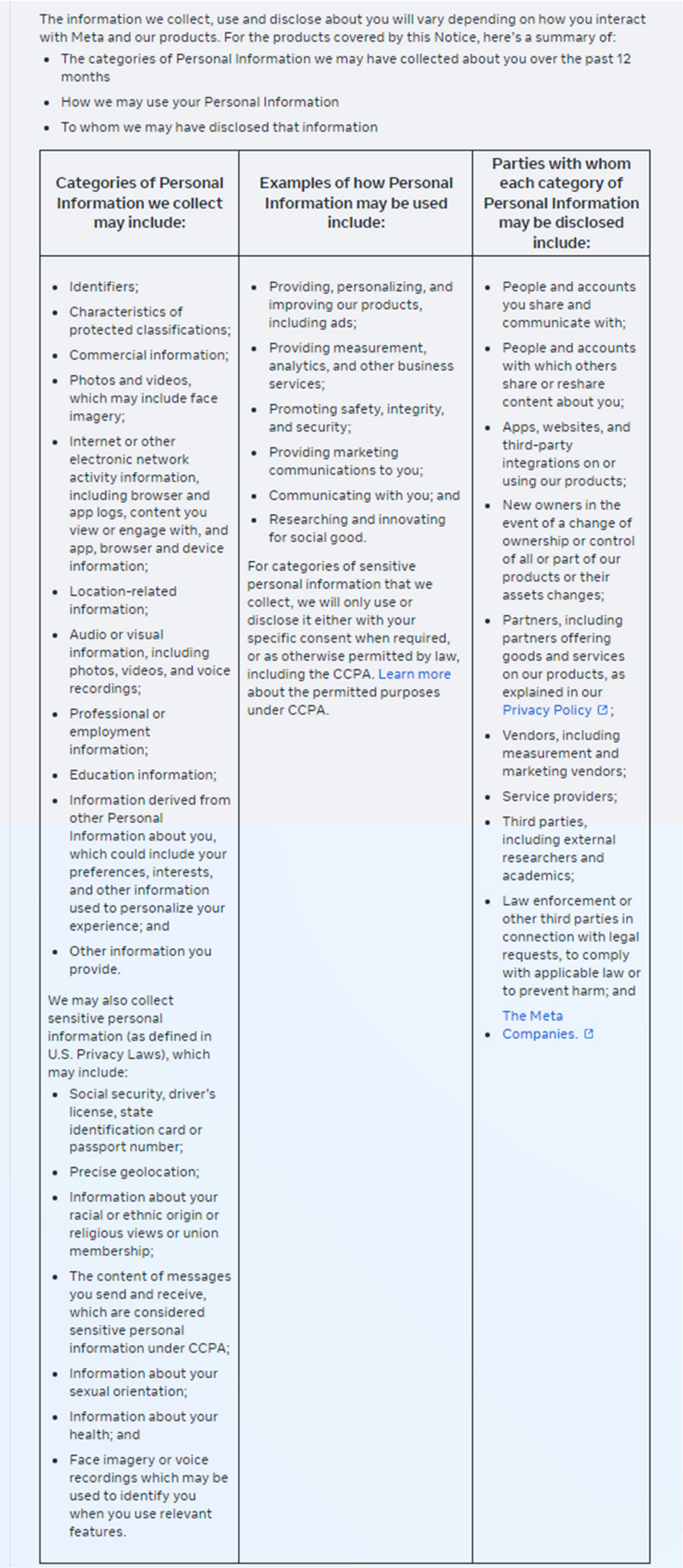
- Social security, driver's license, state identification card or passport number;
- The content of messages you send and receive;
- Information about your health; and
- Face imagery or ***voice recordings which may be used to identify you when you use relevant features***.[48]

140. This is the first time Meta revealed in any of its communications directed to Meta users, albeit vaguely and not in compliance with BIPA, that it can use audio of voices to identify users.

141. A screenshot showing the statements quoted in paragraphs 137-139 is shown below:[49]

[48] *Id.* (emphasis added)

[49] *Id.*



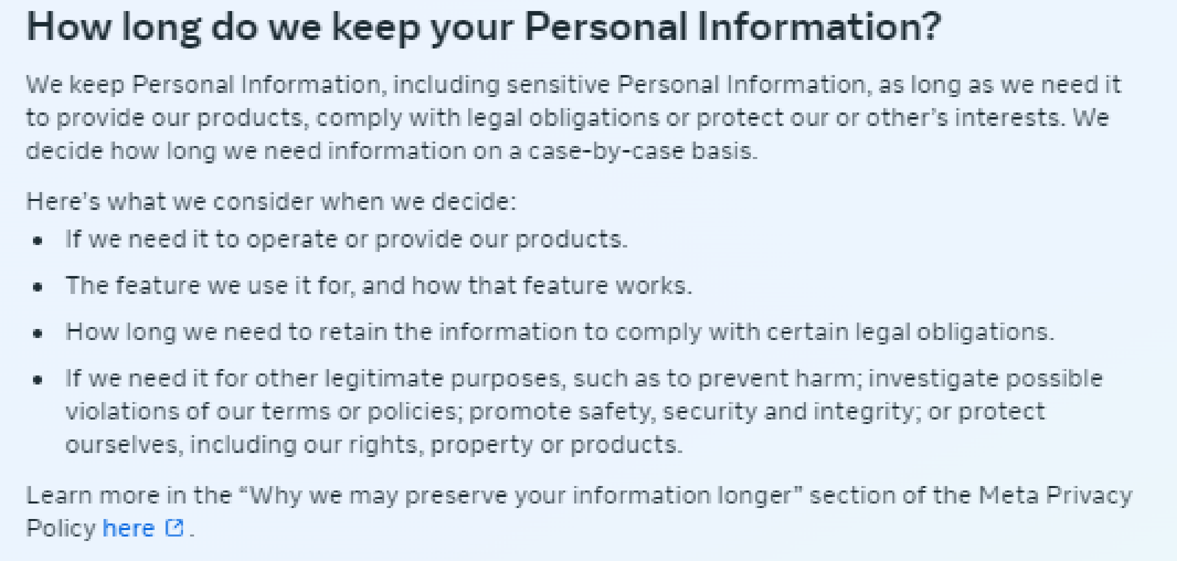
The information we collect, use and disclose about you will vary depending on how you interact with Meta and our products. For the products covered by this Notice, here's a summary of:

- The categories of Personal Information we may have collected about you over the past 12 months
- How we may use your Personal Information
- To whom we may have disclosed that information

Categories of Personal Information we collect may include:	Examples of how Personal Information may be used include:	Parties with whom each category of Personal Information may be disclosed include:
• Identifiers; • Characteristics of protected classifications; • Commercial information; • Photos and videos, which may include face imagery; • Internet or other electronic network activity information, including browser and app logs, content you view or engage with, and app, browser and device information; • Location-related information; • Audio or visual information, including photos, videos, and voice recordings; • Professional or employment information; • Education information; • Information derived from other Personal Information about you, which could include your preferences, interests, and other information used to personalize your experience; and • Other information you provide. We may also collect sensitive personal information (as defined in U.S. Privacy Laws), which may include: • Social security, driver's license, state identification card or passport number; • Precise geolocation; • Information about your racial or ethnic origin or religious views or union membership; • The content of messages you send and receive, which are considered sensitive personal information under CCPA; • Information about your sexual orientation; • Information about your health; and • Face imagery or voice recordings which may be used to identify you when you use relevant features.	• Providing, personalizing, and improving our products, including ads; • Providing measurement, analytics, and other business services; • Promoting safety, integrity, and security; • Providing marketing communications to you; • Communicating with you; and • Researching and innovating for social good. For categories of sensitive personal information that we collect, we will only use or disclose it either with your specific consent when required, or as otherwise permitted by law, including the CCPA. Learn more about the permitted purposes under CCPA.	• People and accounts you share and communicate with; • People and accounts with which others share or reshare content about you; • Apps, websites, and third-party integrations on or using our products; • New owners in the event of a change of ownership or control of all or part of our products or their assets changes; • Partners, including partners offering goods and services on our products, as explained in our Privacy Policy ; • Vendors, including measurement and marketing vendors; • Service providers; • Third parties, including external researchers and academics; • Law enforcement or other third parties in connection with legal requests, to comply with applicable law or to prevent harm; and • The Meta Companies.

142. Meta does not have a written retention schedule or guidelines for permanently destroying biometric identifiers and biometric information by the earlier of (a) when the initial purpose for collecting or obtaining them has been satisfied or (b) within 3 years of the person's last interaction with Meta.

143. Rather, as shown in the screenshot below, the U.S. Privacy Notice indicates that Meta will "keep Personal Information, including sensitive Personal Information, as long as we need it to provide our products, comply with legal obligations or protect our or other's interests. We decide how long we need information on a case-by-case basis."[50]



How long do we keep your Personal Information?

We keep Personal Information, including sensitive Personal Information, as long as we need it to provide our products, comply with legal obligations or protect our or other's interests. We decide how long we need information on a case-by-case basis.

Here's what we consider when we decide:

- If we need it to operate or provide our products.
- The feature we use it for, and how that feature works.
- How long we need to retain the information to comply with certain legal obligations.
- If we need it for other legitimate purposes, such as to prevent harm; investigate possible violations of our terms or policies; promote safety, security and integrity; or protect ourselves, including our rights, property or products.

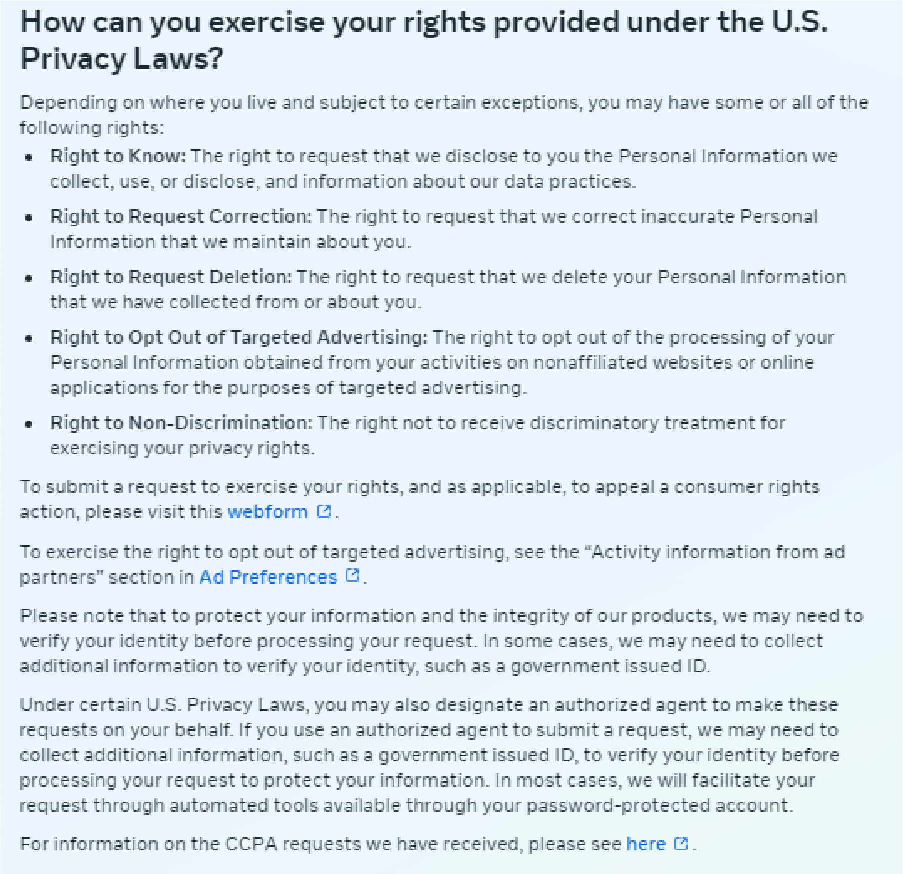
Learn more in the "Why we may preserve your information longer" section of the Meta Privacy Policy here.

144. The U.S. Privacy Notice does not seek any affirmative assent prior to obtaining voiceprints or related biometric data of Illinois residents.

145. Rather, as shown in the screenshot below, the U.S. Privacy Policy indicates opt-out requests and other actions a user must take to limit the use of biometric data (assuming he or she knows it is being collected).[51]

[50] *Id.*

[51] *Id.*



How can you exercise your rights provided under the U.S. Privacy Laws?

Depending on where you live and subject to certain exceptions, you may have some or all of the following rights:

- **Right to Know:** The right to request that we disclose to you the Personal Information we collect, use, or disclose, and information about our data practices.
- **Right to Request Correction:** The right to request that we correct inaccurate Personal Information that we maintain about you.
- **Right to Request Deletion:** The right to request that we delete your Personal Information that we have collected from or about you.
- **Right to Opt Out of Targeted Advertising:** The right to opt out of the processing of your Personal Information obtained from your activities on nonaffiliated websites or online applications for the purposes of targeted advertising.
- **Right to Non-Discrimination:** The right not to receive discriminatory treatment for exercising your privacy rights.

To submit a request to exercise your rights, and as applicable, to appeal a consumer rights action, please visit this webform.

To exercise the right to opt out of targeted advertising, see the "Activity information from ad partners" section in Ad Preferences.

Please note that to protect your information and the integrity of our products, we may need to verify your identity before processing your request. In some cases, we may need to collect additional information to verify your identity, such as a government issued ID.

Under certain U.S. Privacy Laws, you may also designate an authorized agent to make these requests on your behalf. If you use an authorized agent to submit a request, we may need to collect additional information, such as a government issued ID, to verify your identity before processing your request to protect your information. In most cases, we will facilitate your request through automated tools available through your password-protected account.

For information on the CCPA requests we have received, please see here.

146. BIPA, however, does not require Illinois residents to take action to stop or limit the collection and use of biometric data; rather, it requires Meta to obtain their informed consent and make other disclosures *before* it collects such data.

147. Meta's failures to comply with BIPA as set forth herein violated Plaintiff's and the Class Members' privacy rights, and the harm to Plaintiff and the Class occurred in Illinois. *See Cothron*, 477 F. Supp.3d at 732 n.7; *In re Facebook Biometric Info. Privacy Litig.*, 326 F.R.D. 535, 547–48 (N.D. Cal. 2018).

VI. Plaintiff's Experience

148. Plaintiff has a Facebook account and utilizes Meta's Messenger app.

149. On multiple occasions in 2023, 2022, and throughout the Class Period, Plaintiff has, for personal use, input her voice into an audio function on Facebook or Messenger,

including, *inter alia*, to dictate text messages to send via Messenger, sending an audio recording of her voice via Messenger, and making audio calls via Messenger.

150. Plaintiff believes that on other occasions during the Class Period, her voice has been captured by Meta via other users utilizing Facebook or Messenger and/or via third parties.

151. During the Class Period, Meta created, collected, captured, received through trade, stored, and/or otherwise obtained Plaintiff's voiceprint and related biometric information.

152. Meta did not receive a written release, executed by Plaintiff, before it created, collected, captured, received through trade, stored, and/or otherwise obtained Plaintiff's voiceprint and related biometric information.

CLASS ACTION ALLEGATIONS

153. Plaintiff brings this class action on behalf of herself and all others similarly situated, as representative of the following class:

> All natural persons in Illinois from whom Meta created, collected, captured, received, obtained, or stored Digital Voice Data, Voice Characteristics, and/or a Voice Profile.

154. Excluded from the Class is any Defendant, its parents, subsidiaries, affiliates, predecessors, successors, officers, directors, and the immediate family members of such persons. Also excluded are any trial judge who may preside over this action, court personnel and their family members and any juror assigned to this action.

155. Plaintiff is a member of the Class she seeks to represent.

156. Plaintiff reserves the right to amend or modify the Class definitions with greater specificity or division into subclasses after having had an opportunity to conduct discovery.

157. The Class Period is that period within the statute of limitations for this action and extending until a Class is certified herein.

158. The Class is certifiable under Fed. R. Civ. P. 23.

159. **Numerosity.** The members of the Class are so numerous that joinder of all members is impracticable. The determination of the numerosity factor can be made from Defendant's records.

160. **Typicality.** Plaintiff's claims are typical of the claims of the Class Members. Plaintiff and all Class Members have had their rights under BIPA violated based on Meta's failure to comply with the provisions of BIPA.

161. **Commonality and Predominance**. There are questions of law and fact common to the Class, which predominate over any questions affecting individual members of the Class. These common questions of law and fact include, without limitation:

a. Whether Meta possessed, created, collected, captured, received through trade, stored, or otherwise obtained biometric identifiers or biometric information of Plaintiff and the Class;

b. Whether Meta developed, made available to the public, and complied with a retention and destruction policy in compliance with 740 ILCS 14/15(a);

c. Whether Meta informed Plaintiff and the Class in writing that it was collecting their biometric identifiers or biometric information in compliance with 740 ILCS 14/15(b)(1);

d. Whether Meta informed Plaintiff and the Class in writing of the specific purpose and length of term for which it was collecting their biometric identifiers or biometric information in compliance with 740 ILCS 14/15(b)(2);

e. Whether Meta received written releases executed by Plaintiff and the Class before capturing, collecting, receiving through trade, or otherwise obtaining their biometric identifiers or biometric information in compliance with 740 ILCS 14/15(b)(3);

f. Whether Meta sold, leased, traded, or otherwise profited from the biometric identifiers or biometric information of Plaintiff and the Class;

g. Whether Meta stored, transmitted, and protected from disclosure all biometric identifiers and biometric information of Plaintiff and the Class using the reasonable standard of care within the industry in compliance with 740 ILCS 14/15(e)(1);

h. Whether Meta stored, transmitted, and protected from disclosure all biometric identifiers and biometric information of Plaintiff and the Class in a manner that is the same as or more protective than the manner in which it stores, transmits, and protects other confidential and sensitive information in compliance with 740 ILCS 14/15(e)(2); and/or

i. Whether any violations of BIPA by Meta were reckless, intentional, or negligent.

162. **Adequacy**. Plaintiff is a member of the Class she seeks to represent, is committed to the vigorous prosecution of this action, and has retained competent counsel experienced in the prosecution of class actions. Accordingly, Plaintiff is an adequate representative and will fairly and adequately protect the interests of the Class.

163. **Superiority.** A class action is an appropriate method for the fair and efficient adjudication of this controversy and is superior to all other available methods. Because the amount of each individual Class member's claim is small relative to the complexity of the

litigation, and due to the financial resources of Defendant, no Class member could afford to seek legal redress individually for the claims alleged herein. Therefore, absent a class action, Class members will continue to suffer harm and Defendant's misconduct will proceed without remedy. Even if Class members could afford such individual litigation, the court system could not. Given the complex legal and factual issues involved, individualized litigation would significantly increase the delay and expense to all parties and to the Court. Individualized litigation would also create the potential for inconsistent or contradictory rulings. By contrast, a class action presents far fewer management difficulties, allows claims to be heard that might otherwise go unheard because of the relative expense of bringing individual lawsuits, and provides the benefits of adjudication, economies of scale, and comprehensive supervision by a single court. Finally, Plaintiff knows of no difficulty that will be encountered in the management of this litigation that would preclude its maintenance as a class action.

164. **Class Action on Limited Issues.** Because there are common individual issues among the Class, it is appropriate for this action to be maintained as a class action with respect to particular issues if necessary. *See* Fed. R. Civ. P. 23(c)(4).

CLAIMS FOR RELIEF

COUNT I

Meta's Violations of the Biometric Information Privacy Act, 740 ILCS 14/15(a)

165. Plaintiff incorporates by reference each and every allegation set forth above.

166. Meta is a "private entity" under BIPA. 740 ILCS 14/10.

167. During the Class Period, Meta has been in possession of the voiceprints and related biometric information of Plaintiff and the Class.

168. During the Class Period, Meta did not develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric

identifiers and biometric information to occur by the earlier of: (a) when the original purpose for collecting or obtaining such identifiers has been satisfied, or (b) within 3 years of the individual's last interaction with the private entity, as required by 740 ILCS 14/15(a).

169. Instead, Meta's stated policy was that it would retain any data it collected, including sensitive personal information, "as long as we need it to provide our products, comply with legal obligations or protect our or other's interests" and that "[w]e decide how long we need information."

170. Thus, Meta has failed to comply with a retention/destruction policy that conforms to BIPA § 15(a) and has unlawfully retained biometric identifiers and biometric information of Plaintiff and the Class.

171. In violating BIPA, a law in effect since 2008, Meta acted, and continues to act, recklessly and/or intentionally. At the least, Meta negligently violated BIPA.

172. Plaintiff and the Class Members are "aggrieved" under BIPA based on Meta's violation of their rights under BIPA, and accordingly are entitled to seek damages and relief provided for under the statute. *See Rosenbach*, 2019 IL 123186, ¶ 40.

173. Meta's failure to maintain and comply with data retention and destruction protocols harmed, or posed a material risk of harm to, the concrete privacy interests of Plaintiff and the Class, including the right to make informed choices about the use of and control over their inherently sensitive biometric data and to be free from unlawful retention of such sensitive data.

174. Plaintiff and the Class Members seek, *inter alia*, statutory damages of $5,000 per intentional or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), statutory damages of $1,000 per negligent violation of BIPA pursuant to 740 ILCS 14/20(1), and reasonable attorneys' fees and costs pursuant to 740 ILCS 14/20(3).

WHEREFORE, Plaintiff and the Class pray for the relief requested in the Prayer for Relief set forth below.

COUNT II

Meta's Violations of the Biometric Information Privacy Act, 740 ILCS 14/15(b)

175. Plaintiff incorporates by reference each and every allegation set forth above.

176. During the Class Period, Meta collected, captured, received through trade, and/or otherwise obtained the voiceprints and related biometric information of Plaintiff and the Class.

177. Plaintiff and the Class did not execute a written release related to Meta's collection, capturing, purchasing, receiving through trade, or otherwise obtaining their voiceprints or related biometric information.

178. During the Class Period, Meta did not properly inform Plaintiff and the Class in writing that their biometric identifiers and/or biometric information was being collected and/or stored, nor did it inform them in writing of the specific purpose and length of term for which their biometric identifiers and/or biometric information were being collected, stored, and used as required by 740 ILCS 14/15(b)(1)-(2).

179. During the Class Period, Meta systematically and intentionally collected, obtained, used, and/or stored the biometric identifiers and/or biometric information of Plaintiff and the Class without first obtaining from Plaintiff and the Class Members the specific executed written release required by 740 ILCS 14/15(b)(3).

180. In violating BIPA, a law in effect since 2008, Meta acted, and continues to act, recklessly and/or intentionally. At the least, Meta negligently violated BIPA.

181. Plaintiff and the Class Members are "aggrieved" under BIPA based on Meta's violation of their rights under BIPA, and accordingly are entitled to seek damages and relief provided for under the statute. *See Rosenbach*, 2019 IL 123186, ¶ 40.

182. Meta's failure to disclose its practices and obtain the informed consent of Plaintiff and the Class Members before collecting, capturing, receiving through trade, and/or otherwise obtaining their biometric data harmed, or posed a material risk of harm to, the concrete privacy interests of Plaintiff and the Class, including the right to make informed choices about the use of and control over their inherently sensitive biometric data and to be free from the unlawful collection of such sensitive data.

183. Plaintiff and the Class Members seek, *inter alia*, statutory damages of $5,000 per intentional or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), statutory damages of $1,000 per negligent violation of BIPA pursuant to 740 ILCS 14/20(1), and reasonable attorneys' fees and costs pursuant to 740 ILCS 14/20(3).

WHEREFORE, Plaintiff and the Class pray for the relief requested in the Prayer for Relief set forth below.

COUNT III

Meta's Violations of the Biometric Information Privacy Act, 740 ILCS 14/15(c)

184. Plaintiff incorporates by reference each and every allegation set forth above.

185. As set forth above, during the Class Period, Meta used the biometric identifiers and/or biometric information of Plaintiff and the Class that was in its possession to improve Meta's natural language understanding, machine learning, and for its own commercial purposes.

186. Meta's use of the biometric identifiers and biometric information of Plaintiff and the Class to improve Meta's natural language understanding and machine learning, expand the scope of Meta's products, provide targeted content and advertising, and create other business opportunities for Meta has allowed Meta to profit through increased sales of its improved voice-recognition products and services that utilize voice-recognition, and increased targeting of its advertisements for which it receives most of its annual revenue.

187. Moreover, Meta has profited from linking the voiceprints in its possession to Plaintiff and the Class's Facebook profiles and other activities involving Meta.

188. Furthermore, Meta has used the biometric identifiers and biometric information of Plaintiff and the Class to create technology that is so intertwined with the biometric data that marketing the Meta voice-recognition technology and targeted content that utilizes it is essentially disseminating biometric data for profit.

189. Additionally, Meta has used the biometric identifiers and biometric information of Plaintiff and the Class to obtain a competitive advantage over other businesses offering similar devices that provide similar voice-based services and targeted advertising as Meta.

190. Accordingly, Meta violated 740 ILCS 14/15(c) by selling, leasing, trading, or otherwise profiting from Plaintiff's and Class Members' biometric identifiers and/or biometric information in its possession.

191. In violating BIPA, a law in effect since 2008, Meta acted, and continues to act, recklessly and/or intentionally. At the least, Meta negligently violated BIPA.

192. Plaintiff and the Class Members are "aggrieved" under BIPA based on Meta's violation of their rights under BIPA, and accordingly are entitled to seek damages and relief provided for under the statute. *See Rosenbach*, 2019 IL 123186, ¶ 40.

193. Meta's selling, leasing, trading, or otherwise profiting from Plaintiff's and Class Members' biometric identifiers and/or biometric information in its possession harmed, or posed a material risk of harm to, the concrete privacy interests of Plaintiff and the Class, including the right to manage the collection of, use of, and control over inherently sensitive biometric data in the possession of others.

194. Plaintiff and the Class Members seek, *inter alia*, statutory damages of $5,000 per intentional or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), statutory damages of

$1,000 per negligent violation of BIPA pursuant to 740 ILCS 14/20(1), and reasonable attorneys' fees and costs pursuant to 740 ILCS 14/20(3).

WHEREFORE, Plaintiff and the Class pray for the relief requested in the Prayer for Relief set forth below.

COUNT IV

Meta's Violations of the Biometric Information Privacy Act, 740 ILCS 14/15(e)

195. Plaintiff incorporates by reference each and every allegation set forth above.

196. During the Class Period, Meta has failed to store, transmit, and protect from disclosure the biometric identifiers and/or biometric information of Plaintiff and the Class using the reasonable standard of care within the industry, in violation of 740 ILCS 14/15(e)(1).

197. Additionally, during the Class Period, Meta has failed to store, transmit, and protect from disclosure the biometric identifiers and/or biometric information of Plaintiff and the Class in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

198. For example, as set forth above, Meta acknowledges that its large size and vast amount of user data makes it a key target for cyber-attacks, has disclosed it has been the subject of cyber-attacks in the past, states it will be subject to future intrusions, and admits it may not be aware of or discover all such intrusions.

199. In violating BIPA, a law in effect since 2008, Meta acted, and continues to act, recklessly and/or intentionally. At the least, Meta negligently violated BIPA.

200. Plaintiff and the Class Members are "aggrieved" under BIPA based on Meta's violation of their rights under BIPA, and accordingly are entitled to seek damages and relief provided for under the statute. *See Rosenbach*, 2019 IL 123186, ¶ 40.

201. Meta's failure to properly store the biometric data of Plaintiff and the Class Members harmed, or posed a material risk of harm to, the concrete privacy interests of Plaintiff and the Class, including the right to manage the storage of, and control over, inherently sensitive biometric data in the possession of others.

202. Plaintiff and the Class Members seek, *inter alia*, statutory damages of $5,000 per intentional or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), statutory damages of $1,000 per negligent violation of BIPA pursuant to 740 ILCS 14/20(1), and reasonable attorneys' fees and costs pursuant to 740 ILCS 14/20(3).

WHEREFORE, Plaintiff and the Class pray for the relief requested in the Prayer for Relief set forth below.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class, pray for judgment against Defendant as follows:

A. entering an order certifying the Class and appointing Plaintiff as their representative as requested herein, and appointing the undersigned as counsel for the Class;

B. awarding statutory damages of $5,000 for each willful and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1);

C. enjoining Meta from creating, collecting, obtaining, storing, using, selling, leasing, trading, and profiting from Plaintiff's and the Class's biometric identifiers and biometric information until done so in compliance with BIPA;

D. awarding Plaintiff reasonable attorneys' fees, costs, and other expenses pursuant to 740 ILCS 14/20(3);

E. awarding Plaintiff pre-judgment and post-judgment interest, as provided by law; and

F. awarding such other and further relief as is just and appropriate.

Dated: August 16, 2023 **ARIAS SANGUINETTI WANG & TORRIJOS LLP**

By: */s/ Mike Arias*
MIKE ARIAS
ELISE R. SANGUINETTI
ARNOLD C. WANG
CRAIG S. MOMITA
M. ANTHONY JENKINS

GOLDENBERG HELLER & ANTOGNOLI, P.C.
THOMAS P. ROSENFELD
KEVIN P. GREEN
THOMAS C. HORSCROFT

Attorneys for Plaintiff

JURY DEMAND

Plaintiff demands a trial by jury on all claims so triable.

Dated: August 16, 2023 **ARIAS SANGUINETTI WANG & TORRIJOS LLP**

By: */s/ Mike Arias*
MIKE ARIAS
ELISE R. SANGUINETTI
ARNOLD C. WANG
CRAIG S. MOMITA
M. ANTHONY JENKINS

GOLDENBERG HELLER & ANTOGNOLI, P.C.
THOMAS P. ROSENFELD
KEVIN P. GREEN
THOMAS C. HORSCROFT

Attorneys for Plaintiff

JS-CAND 44 (Rev. 10/2020)

CIVIL COVER SHEET

The JS-CAND 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

NATALIE TURCK

(b) County of Residence of First Listed Plaintiff St. Clair, IL
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
ARIAS SANGUINETTI WANG & TORRIJOS, LLP Telephone: (310) 844-9696
Mike Arias, Esq. (SBN 115385)
6701 Center Drive West, Suite 1400, Los Angeles, California 90045

DEFENDANTS

META PLATFORMS, INC.

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

☐ 1 U.S. Government Plaintiff
☐ 3 Federal Question *(U.S. Government Not a Party)*
☐ 2 U.S. Government Defendant
☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☒ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT

☐ 110 Insurance
☐ 120 Marine
☐ 130 Miller Act
☐ 140 Negotiable Instrument
☐ 150 Recovery of Overpayment Of Veteran's Benefits
☐ 151 Medicare Act
☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
☐ 153 Recovery of Overpayment of Veteran's Benefits
☐ 160 Stockholders' Suits
☐ 190 Other Contract
☐ 195 Contract Product Liability
☐ 196 Franchise

REAL PROPERTY

☐ 210 Land Condemnation
☐ 220 Foreclosure
☐ 230 Rent Lease & Ejectment
☐ 240 Torts to Land
☐ 245 Tort Product Liability
☐ 290 All Other Real Property

TORTS

PERSONAL INJURY

☐ 310 Airplane
☐ 315 Airplane Product Liability
☐ 320 Assault, Libel & Slander
☐ 330 Federal Employers' Liability
☐ 340 Marine
☐ 345 Marine Product Liability
☐ 350 Motor Vehicle
☐ 355 Motor Vehicle Product Liability
☒ 360 Other Personal Injury
☐ 362 Personal Injury -Medical Malpractice

CIVIL RIGHTS

☐ 440 Other Civil Rights
☐ 441 Voting
☐ 442 Employment
☐ 443 Housing/ Accommodations
☐ 445 Amer. w/Disabilities–Employment
☐ 446 Amer. w/Disabilities–Other
☐ 448 Education

PERSONAL INJURY

☐ 365 Personal Injury – Product Liability
☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY

☐ 370 Other Fraud
☐ 371 Truth in Lending
☐ 380 Other Personal Property Damage
☐ 385 Property Damage Product Liability

PRISONER PETITIONS

HABEAS CORPUS

☐ 463 Alien Detainee
☐ 510 Motions to Vacate Sentence
☐ 530 General
☐ 535 Death Penalty

OTHER

☐ 540 Mandamus & Other
☐ 550 Civil Rights
☐ 555 Prison Condition
☐ 560 Civil Detainee– Conditions of Confinement

FORFEITURE/PENALTY

☐ 625 Drug Related Seizure of Property 21 USC § 881
☐ 690 Other

LABOR

☐ 710 Fair Labor Standards Act
☐ 720 Labor/Management Relations
☐ 740 Railway Labor Act
☐ 751 Family and Medical Leave Act
☐ 790 Other Labor Litigation
☐ 791 Employee Retirement Income Security Act

IMMIGRATION

☐ 462 Naturalization Application
☐ 465 Other Immigration Actions

BANKRUPTCY

☐ 422 Appeal 28 USC § 158
☐ 423 Withdrawal 28 USC § 157

PROPERTY RIGHTS

☐ 820 Copyrights
☐ 830 Patent
☐ 835 Patent─Abbreviated New Drug Application
☐ 840 Trademark
☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY

☐ 861 HIA (1395ff)
☐ 862 Black Lung (923)
☐ 863 DIWC/DIWW (405(g))
☐ 864 SSID Title XVI
☐ 865 RSI (405(g))

FEDERAL TAX SUITS

☐ 870 Taxes (U.S. Plaintiff or Defendant)
☐ 871 IRS–Third Party 26 USC § 7609

OTHER STATUTES

☐ 375 False Claims Act
☐ 376 Qui Tam (31 USC § 3729(a))
☐ 400 State Reapportionment
☐ 410 Antitrust
☐ 430 Banks and Banking
☐ 450 Commerce
☐ 460 Deportation
☐ 470 Racketeer Influenced & Corrupt Organizations
☐ 480 Consumer Credit
☐ 485 Telephone Consumer Protection Act
☐ 490 Cable/Sat TV
☐ 850 Securities/Commodities/ Exchange
☐ 890 Other Statutory Actions
☐ 891 Agricultural Acts
☐ 893 Environmental Matters
☐ 895 Freedom of Information Act
☐ 896 Arbitration
☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding
☐ 2 Removed from State Court
☐ 3 Remanded from Appellate Court
☐ 4 Reinstated or Reopened
☐ 5 Transferred from Another District *(specify)*
☐ 6 Multidistrict Litigation–Transfer
☐ 8 Multidistrict Litigation–Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d)

Brief description of cause:
Violation of Illinois' Biometric Information Privacy Act, 740 ILCS 14/1 et seq.

VII. REQUESTED IN COMPLAINT:

☑ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, Fed. R. Civ. P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S), IF ANY *(See instructions)*:

JUDGE

DOCKET NUMBER

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)

(Place an "X" in One Box Only) ☒ **SAN FRANCISCO/OAKLAND** ☐ **SAN JOSE** ☐ **EUREKA-MCKINLEYVILLE**

DATE 08/16/2023

SIGNATURE OF ATTORNEY OF RECORD */s/ Mike Arias*

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS-CAND 44

Authority For Civil Cover Sheet. The JS-CAND 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I. a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)."

II. Jurisdiction. The basis of jurisdiction is set forth under Federal Rule of Civil Procedure 8(a), which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.

(1) United States plaintiff. Jurisdiction based on 28 USC §§ 1345 and 1348. Suits by agencies and officers of the United States are included here.

(2) United States defendant. When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.

(3) Federal question. This refers to suits under 28 USC § 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.

(4) Diversity of citizenship. This refers to suits under 28 USC § 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked**.** (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS-CAND 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

V. Origin. Place an "X" in one of the six boxes.

(1) Original Proceedings. Cases originating in the United States district courts.

(2) Removed from State Court. Proceedings initiated in state courts may be removed to the district courts under Title 28 USC § 1441. When the petition for removal is granted, check this box.

(3) Remanded from Appellate Court. Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.

(4) Reinstated or Reopened. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

(5) Transferred from Another District. For cases transferred under Title 28 USC § 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.

(6) Multidistrict Litigation Transfer. Check this box when a multidistrict case is transferred into the district under authority of Title 28 USC § 1407. When this box is checked, do not check (5) above.

(8) Multidistrict Litigation Direct File. Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket.

Please note that there is no Origin Code 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC § 553. Brief Description: Unauthorized reception of cable service.

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Federal Rule of Civil Procedure 23.

Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.

Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS-CAND 44 is used to identify related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

IX. Divisional Assignment. If the Nature of Suit is under Property Rights or Prisoner Petitions or the matter is a Securities Class Action, leave this section blank. For all other cases, identify the divisional venue according to Civil Local Rule 3-2: "the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated."

Date and Attorney Signature. Date and sign the civil cover sheet.