

GIBSON, DUNN & CRUTCHER LLP
 LAUREN R. GOLDMAN (*pro hac vice*)
 lgoldman@gibsondunn.com
 200 Park Avenue
 New York, NY 10166
 Telephone: (212) 351-4000
 Facsimile: (212) 351-4035

ELIZABETH K. MCCLOSKEY (SBN 268184)
 emccloskey@gibsondunn.com
 ABIGAIL A. BARRERA (SBN 301746)
 abarrera@gibsondunn.com
 555 Mission Street, Suite 3000
 San Francisco, CA 94105
 Telephone: (415) 393-8200
 Facsimile: (415) 393-8306

TRENTON J. VAN OSS (*pro hac vice*)
 tvanoss@gibsondunn.com
 1050 Connecticut Avenue, N.W.
 Washington, DC 20036-5306
 Telephone: (202) 955-8500
 Facsimile: (202) 467-0539

*Attorneys for Defendant Meta Platforms, Inc.
 (formerly known as Facebook, Inc.)*

COOLEY LLP
 MICHAEL G. RHODES (SBN 116127)
 rhodesmg@cooley.com
 KYLE C. WONG (SBN 224021)
 kwong@cooley.com
 CAMERON J. CLARK (SBN 313039)
 cclark@cooley.com
 CAROLINE A. LEBEL (SBN 340067)
 clebel@cooley.com
 3 Embarcadero Center, 20th Floor
 San Francisco, CA 94111-4004
 Telephone: (415) 693-2000
 Facsimile: (415) 693-2222

UNITED STATES DISTRICT COURT
 NORTHERN DISTRICT OF CALIFORNIA
 SAN FRANCISCO DIVISION

IN RE META PIXEL HEALTHCARE
 LITIGATION

 This Document Relates To:
 Case No. 3:22-cv-3580-WHO (Doe)

Case No. 3:22-cv-3580-WHO

PUTATIVE CLASS ACTION

**DEFENDANT META PLATFORMS, INC.'S
 OPPOSITION TO PLAINTIFFS' MOTION
 FOR PRELIMINARY INJUNCTION**

*[Declarations of Tobias Wooldridge and Abigail
 A. Barrera filed concurrently herewith]*

Action Filed: June 17, 2022

Honorable Judge William H. Orrick

Date: November 9, 2022

Time: 2:00 p.m.

Location: Courtroom 2, 17th Floor

TABLE OF CONTENTS

	<u>Page</u>
INTRODUCTION	1
BACKGROUND	2
A. Meta’s Policies	3
B. Meta’s Restrictions On Use Of The Pixel Tool	6
C. Previous Litigation	7
D. Procedural History	8
LEGAL STANDARD.....	9
ARGUMENT	10
I. The Planned Consolidated Amended Complaint Moots Plaintiffs’ Motion.	10
II. Plaintiffs Cannot Meet Their Heavy Burden To Justify A Preliminary Injunction.	11
A. Plaintiffs Will Not Suffer Irreparable Harm Absent A Preliminary Injunction.	11
B. The Balance Of Equities Does Not Tip In Plaintiffs’ Favor.....	13
C. A Preliminary Injunction Is Not In The Public Interest.....	14
D. Plaintiffs Are Unlikely To Succeed On The Merits.....	15
1. Consent bars all of plaintiffs’ claims.	15
2. Each of plaintiffs’ claims also fails for multiple other reasons.....	20
III. Plaintiffs’ Requested Relief Is Impermissibly Overbroad.	24
CONCLUSION	25

TABLE OF AUTHORITIES

Cases	Page(s)
<i>Adtrader, Inc. v. Google LLC</i> , 2018 WL 1876950 (N.D. Cal. Apr. 19, 2018)	12
<i>Al Otro Lado v. Wolf</i> , 952 F.3d 999 (9th Cir. 2020).....	12
<i>Amoco Prod. Co. v. Vill. of Gambell</i> , 480 U.S. 531 (1987).....	13
<i>Astra USA, Inc. v. Santa Clara Cnty.</i> , 563 U.S. 110 (2011).....	18
<i>Barrilleaux v. Mendocino Cnty.</i> , 2016 WL 4269328 (N.D. Cal. Aug. 15, 2016).....	10
<i>Bernhardt v. Los Angeles Cnty.</i> , 339 F.3d 920 (9th Cir. 2003).....	14
<i>Brien v. J.P. Morgan Chase Bank, N.A.</i> , 2010 WL 11597807 (C.D. Cal. Nov. 24, 2010).....	12
<i>Brodsky v. Apple Inc.</i> , 445 F. Supp. 3d 110 (N.D. Cal. 2020)	21
<i>Brown v. Google LLC</i> , 525 F. Supp. 3d 1049 (N.D. Cal. 2021)	22
<i>California v. Azar</i> , 911 F.3d 558 (9th Cir. 2018).....	24
<i>Clay v. Wells Fargo Home Mortg., N.A.</i> , 2013 WL 1189712 (E.D. Cal. Mar. 21, 2013)	10
<i>Cline v. Reetz-Laiolo</i> , 329 F. Supp. 3d 1000 (N.D. Cal. 2018)	21
<i>Cuyler v. United States</i> , 362 F.3d 949 (7th Cir. 2004).....	18
<i>Doe v. Va. Mason Med. Ctr.</i> , 2020 WL 1983046 (Wash. Sup. Ct. Feb. 12, 2020).....	13
<i>In re DoubleClick Inc. Privacy Litig.</i> , 154 F. Supp. 2d 497 (S.D.N.Y. 2001).....	20
<i>Easyriders Freedom F.I.G.H.T. v. Hannigan</i> , 92 F.3d 1486 (9th Cir. 1996).....	24
<i>Envtl. Democracy Project v. Green Sage Mgmt., LLC</i> , 2022 WL 4596616 (N.D. Cal. Aug. 23, 2022).....	13

1	<i>F.B.T. Prods., LLC v. Aftermath Records</i> ,	
2	621 F.3d 958 (9th Cir. 2010).....	17, 20
3	<i>In re Facebook, Inc. Internet Tracking Litig.</i> ,	
4	956 F.3d 589 (9th Cir. 2020).....	22, 24
5	<i>Falck N. Cal. Corp. v. Scott Griffith Collaborative Sols., LLC</i> ,	
6	25 F.4th 763 (9th Cir. 2022)	11
7	<i>Fogelstrom v. Lamps Plus, Inc.</i> ,	
8	195 Cal. App. 4th 986 (Cal. Ct. App. 2011)	23
9	<i>Garcia v. Google, Inc.</i> ,	
10	786 F.3d 733 (9th Cir. 2015) (en banc).....	2, 10, 11, 15
11	<i>Garcia v. Mid-Atl. Military Family Communities LLC</i> ,	
12	2021 WL 1429474 (E.D. Va. Mar. 4, 2021)	10
13	<i>Geisert v. Brown</i> ,	
14	No. 3:9-cv-670 (N.D. Tex. Mar. 22, 2010).....	10
15	<i>In re Google Inc.</i> ,	
16	2013 WL 5423918	22
17	<i>In re Google Inc. Gmail Litig.</i> ,	
18	2014 WL 1102660 (N.D. Cal. Mar. 18, 2014).....	20
19	<i>In re Google, Inc. Privacy Policy Litig.</i> ,	
20	58 F. Supp. 3d 968 (N.D. Cal. 2014)	23
21	<i>Hammerling v. Google LLC</i> ,	
22	2022 WL 2812188 (N.D. Cal. July 18, 2022).....	23, 24
23	<i>Hartmann v. Cal. Dep't of Corr. & Rehab.</i> ,	
24	707 F.3d 1114 (9th Cir. 2013).....	13
25	<i>Hernandez v. Hillsides, Inc.</i> ,	
26	211 P.3d 1063 (Cal. 2009)	22
27	<i>Hill v. Nat'l Coll. Athletic Ass'n</i> ,	
28	865 P.2d 633 (Cal. 1994)	15, 22
	<i>Illinois v. Facebook</i> ,	
	No. 2018 CH 3868 (Ill. Cir. Ct. Mar. 8, 2021)	19
	<i>Krackenberger v. Northwestern Memorial Hosp., et al.</i> ,	
	No. 1:22-cv-04203 (N.D. Ill.)	9
	<i>Lee v. Canada Goose US, Inc.</i> ,	
	2021 WL 2665955 (S.D.N.Y. June 29, 2011).....	19
	<i>Marlyn Nutraceuticals, Inc. v. Mucos Pharma GmbH & Co.</i> ,	
	571 F.3d 873 (9th Cir. 2009).....	10, 11
	<i>McCoy v. Alphabet, Inc.</i> ,	
	2021 WL 405816 (N.D. Cal. Feb. 2, 2021)	23

1	<i>Med. Lab. Mgmt. Consultants v. Am. Broadcasting Cos.,</i>	
2	306 F.3d 806 (9th Cir. 2002).....	23
3	<i>Miller v. Elam,</i>	
4	2011 WL 1549398 (E.D. Cal. Apr. 21, 2011).....	18
5	<i>Miller v. Nat'l Broadcasting Co.,</i>	
6	187 Cal. App. 3d 1463 (Cal. Ct. App. 1986)	23
7	<i>Nat'l Ctr. for Immigrants Rights, Inc. v. I.N.S.,</i>	
8	743 F.2d 1365 (9th Cir. 1984).....	24
9	<i>Naugle, et al. v. Meta Platforms, Inc., et al.,</i>	
10	No. 1:22-cv-00727-UA-JEP (M.D.N.C.).....	9
11	<i>NRDC v. Winter,</i>	
12	508 F.3d 885 (9th Cir. 2007).....	25
13	<i>Oakland Tribune, Inc. v. Chronicle Pub. Co.,</i>	
14	762 F.2d 1374 (9th Cir. 1985).....	11
15	<i>People v. Nakai,</i>	
16	183 Cal. App. 4th 499 (Cal. Ct. App. 2010)	22
17	<i>Perfect 10, Inc. v. Google, Inc.,</i>	
18	653 F.3d 976 (9th Cir. 2011).....	11
19	<i>Perkins v. LinkedIn Corp.,</i>	
20	53 F. Supp. 3d 1190 (N.D. Cal. 2014)	16, 17, 18
21	<i>Price v. City of Stockton,</i>	
22	390 F.3d 1105 (9th Cir. 2004).....	24
23	<i>Ramirez v. Cnty. of San Bernardino,</i>	
24	806 F.3d 1002 (9th Cir. 2015).....	10
25	<i>Revitch v. New Moosejaw, LLC,</i>	
26	2019 WL 5485330 (N.D. Cal. Oct. 23, 2019).....	21
27	<i>Rodriguez v. Google LLC,</i>	
28	2021 WL 2026726 (N.D. Cal. May 21, 2021)	20
	<i>Schulman v. Grp. W Prods., Inc.,</i>	
	955 P.2d 469 (Cal. 1998)	23
	<i>Smidga v. Meta Platforms, Inc., et al.,</i>	
	No. 2:22-cv-01231-MPK (W.D. Pa.).....	9
	<i>Smith v. Facebook, Inc.,</i>	
	262 F. Supp. 3d 943 (N.D. Cal. 2017)	7, 8
	<i>Smith v. Facebook, Inc.,</i>	
	745 F. App'x 8 (9th Cir. 2018)	8, 16, 17, 18
	<i>Stormans, Inc. v. Selecky,</i>	
	586 F.3d 1109 (9th Cir. 2009).....	14

1	<i>Susan S. v. Israels,</i>	
2	55 Cal. App. 4th 1290 (Cal. Ct. App. 1997)	23
3	<i>Sussman v. Am. Broad. Cos., Inc.,</i>	
4	186 F.3d 1200 (9th Cir. 1999).....	20
5	<i>TBG Ins. Servs. Corp. v. Superior Court,</i>	
6	96 Cal. App. 4th 443 (Cal. Ct. App. 2002)	22
7	<i>Techtronic Power Tools Tech. Ltd. v. Harbor Freight Tools USA, Inc.,</i>	
8	No. 8:20-cv-2004 (D.S.C. Oct. 21, 2020)	10
9	<i>Tsao v. Desert Palace, Inc.,</i>	
10	698 F.3d 1128 (9th Cir. 2012).....	17
11	<i>United States v. Holtzman,</i>	
12	762 F.2d 720 (9th Cir. 1985).....	14
13	<i>Webb v. Smart Document Sols., LLC,</i>	
14	499 F.3d 1078 (9th Cir. 2007).....	18
15	<i>Winter v. Nat. Res. Def. Council, Inc.,</i>	
16	555 U.S. 7 (2008).....	9
17	<i>Zhang v. Superior Court,</i>	
18	304 P.3d 163 (Cal. 2013)	18
19	<i>In re Zynga Privacy Litig.,</i>	
20	750 F.3d 1098 (9th Cir. 2014).....	21
21	Statutes	
22	18 U.S.C. § 2510(8)	21
23	18 U.S.C. § 2511	15, 20, 21
24	Cal. Penal Code § 631(a)	15, 21
25	Cal. Penal Code § 632(a)	15, 21
26	Rules	
27	Rule 65(d)	14
28	Regulations	
	45 C.F.R. § 164.502	18
	45 C.F.R. § 164.508	18
	65 Fed. Reg. 82601	18

STATEMENT OF ISSUES TO BE DECIDED

1. Whether plaintiffs’ motion for a preliminary injunction is moot in light of the Court’s consolidation order requiring plaintiffs to file a superseding consolidated amended complaint.
2. Whether “the law and facts *clearly favor* [plaintiffs’] position,” and whether plaintiffs can otherwise satisfy the “doubly demanding” standard for the “particularly disfavored” remedy of a mandatory injunction. *Garcia v. Google, Inc.*, 786 F.3d 733, 740 (9th Cir. 2015) (en banc) (quotation marks and citation omitted).
3. Whether, even assuming plaintiffs could satisfy the standard for a mandatory injunction, the relief plaintiffs seek is impermissibly overbroad.

MEMORANDUM OF POINTS AND AUTHORITIES

INTRODUCTION

Plaintiffs, four Facebook users, allege that their healthcare providers sent sensitive information about them to Meta through a common Internet tool, in violation of both HIPAA and Meta’s policies. They have not sued their healthcare providers; they have sued Meta. They now ask this Court to issue a sweeping preliminary injunction that would bar Meta’s receipt or use of all “patient information and communications” from all “HIPAA-covered entities.” Plaintiffs do not explain how such an injunction would work, given that (1) website developers (not Meta) choose what information they send to Meta, and (2) Meta already takes extensive measures to prevent even *potentially* sensitive data from being sent to it. Nor do plaintiffs allege that before filing their motion they invoked any of the privacy controls Meta provides to users, including the option to disconnect their off-Facebook activity (*i.e.*, the data at issue in this case) from their user accounts. Plaintiffs have put forth no factual or legal justification for the extraordinary relief they seek, and this Court should deny their motion.

This lawsuit challenges the way in which certain healthcare providers use a common Internet tool offered by numerous companies across many industries. Meta’s version of this tool, known as the “Meta Pixel,” is a publicly available piece of code that allows website developers to gather analytics information about people who visit their websites. Developers can choose to install this code on their websites and customize it to measure particular types of activity, such as online purchases. When a person engages in that activity on the developer’s site, information about the specified activity is sent automatically to Meta’s systems, which attempt to match it with a Facebook account. Meta’s systems then send de-identified information back to the web developer, which can use the data to improve its online services. Facebook users consent to the transmission and use of data sent to Meta through the Pixel tool, including for advertising purposes, when they sign up for Facebook and agree to its policies. Users also have the option to (1) disconnect their off-Facebook activity from their Facebook accounts, and (2) disconnect any historical information that has been collected about their off-Facebook activity.

Meta does not want healthcare providers—or any other website developers—to send sensitive data to it. Accordingly, Meta takes extensive measures to prevent developers from transmitting that information, including: (1) contractually requiring them to have the legal right to share any information

1 they send to Meta; (2) contractually prohibiting them from sending any health-related or other sensitive
 2 information to Meta; (3) developing filters that are constantly improving Meta’s ability to screen out
 3 potentially sensitive information that Meta detects; and (4) notifying developers when potentially
 4 sensitive data is detected and instructing them to ensure they are not sending sensitive information.

5 Plaintiffs allege that various healthcare companies nevertheless sent sensitive information about
 6 them to Meta, in violation of the companies’ contractual obligations to Meta and their legal obligations
 7 under HIPAA. Plaintiffs’ claim is that by receiving this information, *Meta* violated state and federal
 8 privacy statutes and common-law doctrines, and breached its promise to users that it would require its
 9 business partners to comply with applicable privacy laws. Months after filing their lawsuit, the
 10 plaintiffs in this case moved for a preliminary injunction that would order Meta to stop receiving and
 11 using *all* “patient information and communications” from *all* “HIPAA-covered entities” using the Meta
 12 Pixel tool.

13 This motion is meritless. Plaintiffs have not come close to demonstrating that the facts and the
 14 law “*clearly favor*” them—the “doubly demanding” prerequisite for an injunction that seeks to change
 15 the status quo. *Garcia v. Google, Inc.*, 786 F.3d 733, 740 (9th Cir. 2015) (en banc). Plaintiffs certainly
 16 cannot show extreme or irreparable harm; injunctive relief is unavailable as a matter of law when (1)
 17 the plaintiffs themselves could, but have not chosen to, prevent the alleged harm from occurring, *or* (2)
 18 the plaintiffs cannot show that their harm resulted from conduct *by the defendant* (as opposed to third-
 19 party web developers). Both are true here. For the same reasons, the balance of equities favors Meta,
 20 and an injunction is not in the public interest. Finally, plaintiffs cannot demonstrate *any* likelihood
 21 (much less a strong likelihood) of success on the merits: the three claims they press in their motion—
 22 under the Electronic Communications Privacy Act, the California Invasion of Privacy Act, and
 23 California privacy tort law—fail, both because plaintiffs consented to the activity they complain about
 24 and because they fail to make out the elements of each claim.

25 BACKGROUND

26 This case centers on a tool called “Pixel” that Meta makes available to third-party website
 27 developers. The Meta Pixel—Meta’s version of a common analytics tool used across the web and
 28 offered by numerous other companies—is a free, publicly available piece of code that third-party

website developers can choose to install and customize on their websites to measure certain actions taken by users on their own sites (*e.g.*, online purchases); this data helps inform and improve the developers' online services. Declaration of Tobias Wooldridge ("Wooldridge Decl.") ¶ 3.¹ The Pixel tool is widely deployed across many industries and is not healthcare-specific. Each developer chooses whether to use this tool (Meta does not obligate anyone to use Pixel) and what user actions to measure, but Meta contractually bars developers from sending sensitive data to it and takes steps to prevent developers from doing so. *Id.* ¶¶ 3–4. Meta also explains to its users how the Pixel works and what it is used for, and gives users the option of disconnecting their off-Facebook activity from their Facebook accounts. *Id.* ¶¶ 11–12; *see also* Declaration of Abigail A. Barrera ("Barrera Decl."), Exs. F, G, H, I.

A. Meta's Policies

Meta operates Facebook, the world's largest social technology company. Compl. ¶ 58.² When users sign up for a Facebook account, they agree to Meta's Terms of Service, Data Policy, and Cookies Policy. *Id.* ¶ 49. Those policies are contractually binding on both Meta and its users, and they contain important disclosures about Facebook and how Meta collects and uses data, including through the Pixel tool. *Id.*³

Terms of Service. The Terms of Service govern the "use of Facebook, Messenger, and the other products, features, apps, services, technologies, and software" Meta offers. Barrera Decl., Ex. A at 1. Meta believes its "services are most useful when people are connected to people, groups, and organizations they care about," and Meta informs users that it "use[s] data about the connections you

¹ When someone takes an action that the developer has chosen to measure on its website, the Meta Pixel is triggered and sends Meta certain data, called an "Event." Wooldridge Decl. ¶ 4. Meta attempts to match the Events it receives to Meta users. *Id.* The developer can then choose to show ads to users who have taken a certain action on their own website. *Id.* But the identity of matched Meta users is not revealed to the developer or to any advertiser. *Id.* Meta can also provide the developer with de-identified, aggregated reporting that helps the developer better understand the impact of its ads by measuring what happens when people see them. *Id.*

² Meta was previously known as "Facebook, Inc." In late 2021, the company changed its name to "Meta Platforms, Inc.," but the social media platform itself is still known as Facebook.

³ Plaintiffs refer to these policies as the "Terms of Use," the "Data Policy," and the "Cookie Policy." Compl. ¶¶ 31, 49; Dkt. 46 ("Mot.") at 4. The Data Policy is now called the "Privacy Policy," but to avoid confusion, this brief uses the version referenced in plaintiffs' complaint and in their motion. The policies are attached as Exhibits A, B, and C to the Barrera declaration, and where a policy has since been updated, the updated versions are attached separately.

1 make, the choices and settings you select, and what you share and do on and off our Products - to
 2 personalize your experience.” *Id.* at 2. The Terms of Service explain that Meta shows users
 3 “personalized ads, offers, and other sponsored or commercial content to help [them] discover content,
 4 products, and services that are offered by the many businesses and organizations that use Facebook and
 5 other Meta Products.” *Id.* at 3. To provide these services, Meta’s terms explain, Meta “collect[s] and
 6 use[s] your personal data.” *Id.* at 5. The terms link to the Data Policy for more information. *Id.* at 1.

7 **Data Policy.** The Data Policy “describes the information [Meta] process[es] to support
 8 Facebook, Instagram, Messenger and other products and features offered by Meta.” Barrera Decl., Ex.
 9 B at 1. Among other things, the Data Policy tells users that “[a]dvertisers, app developers, and
 10 publishers can send us information through Meta Business Tools they use, including our social plug-
 11 ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Meta pixel.” *Id.* at 4. “These
 12 partners,” the policy explains, “provide information about your activities off of our Products—
 13 including information about your device, websites you visit, purchases you make, the ads you see, and
 14 how you use their services—whether or not you have an account or are logged into our Products.” *Id.*
 15 at 4–5. The policy further explains that “[p]artners receive your data when you visit or use their services
 16 or through third parties they work with,” and says that Meta “require[s] each of these partners to have
 17 lawful rights to collect, use and share your data before providing any data to us.” *Id.* at 5.

18 The Data Policy also informs users that Meta uses this information “to personalize features and
 19 content (including your ads, Facebook News Feed, Instagram Feed, and Instagram Stories) and make
 20 suggestions for you.” *Id.*; *see also id.* at 6 (“We use the information we have (including your activity
 21 off our Products, such as the websites you visit and ads you see) to help advertisers and other partners
 22 measure the effectiveness and distribution of their ads and services, and understand the types of people
 23 who use their services and how people interact with their websites, apps, and services.”). Meta does
 24 not, however, “share information that personally identifies” users with advertisers unless users give
 25 permission. *Id.* at 9.

26 **Cookies Policy.** Cookies are “small pieces of text used to store information on web browsers.”
 27 Barrera Decl., Ex. C at 1. They “store and receive identifiers and other information on computers,
 28 phones and other devices,” and they can serve a number of different functions—for example,

1 “personalising content, tailoring and measuring ads, and providing a safer experience.” *Id.* at 1–2.
 2 Meta’s Cookies Policy informs users that Meta “use[s] cookies if you have a Facebook account, use
 3 the Meta Products, including our website and apps, or visit other websites and apps that use the Meta
 4 Products (including the Like button).” *Id.* at 1. Meta explains that cookies allow it to “understand the
 5 information that we receive about you, including information about your use of other websites and
 6 apps, whether or not you are registered or logged in,” and that Meta “use[s] cookies to help us show
 7 ads and to make recommendations for businesses and other organisations to people who may be
 8 interested in the products, services or causes they promote.” *Id.* at 1–2. Cookies allow Meta “to provide
 9 insights about the people who use the Meta Products, as well as the people who interact with the ads,
 10 websites and apps of our advertisers and the businesses that use the Meta Products.” *Id.* at 3. The
 11 policy also describes the cookie used to enable the Meta Pixel (“_fbp”) and explains that Meta’s
 12 “business partners may also choose to share information with Meta from cookies set in their own
 13 websites’ domains, whether or not you have a Facebook account or are logged in.” *Id.* at 4; *see also*
 14 *id.* at 4–5 (“Meta uses cookies and receives information when you visit [websites and apps that use the
 15 Meta Products], including device information and information about your activity, without any further
 16 action from you. This occurs whether or not you have a Facebook account or are logged in.”).

17 ***Business Tools Terms.*** All third-party web developers that use Meta services—including
 18 Meta’s Pixel tool—must agree to the publicly available Business Tools Terms. Consistent with the
 19 Data Policy’s statement that Meta requires partners to “have lawful rights to collect, use and share”
 20 user data, Barrera Decl., Ex. B at 5, the Business Tools Terms require developers to “represent and
 21 warrant that you (and any data provider that you may use) have all of the necessary rights and
 22 permissions and a lawful basis (in compliance with all applicable laws, regulations and industry
 23 guidelines) for the disclosure and use of Business Tool Data.” Barrera Decl., Ex. D at 1. Partners must
 24 also “represent and warrant that [they] have provided robust and sufficiently prominent notice to users
 25 regarding the Business Tool Data collection, sharing and usage,” including a “clear and prominent
 26 notice on each web page where [Meta] pixels are used that links to a clear explanation [of] . . . how
 27 users can opt-out of the collection and use of information for ad targeting.” *Id.* at 3. As a condition of
 28 using the Pixel tool, developers specifically agree that they will “*not share Business Tool Data . . . that*

[they] know or reasonably should know . . . includes health, financial or other categories of sensitive information (including any information defined as sensitive under applicable laws, regulations and applicable industry guidelines).” *Id.* at 2 (emphasis added); *see also* Barrera Decl., Ex. E at 2 (similar provision in Commercial Terms).

User Control. Meta gives users the ability to control the use of information about their off-Facebook activity (such as activity on third-party websites) for advertising purposes. Wooldridge Decl. ¶ 11. The Off-Facebook Activity tool allows users to view a summary of information Meta has received about their activity from third parties through the Business Tools, including Pixel. *Id.* Users can disconnect the off-Facebook activity that has been associated with their account—which prevents the data from being used for personalized advertising—and can turn off storage of any future connections for all third-party websites (or on a website-by-website basis). *Id.* The “Data About Your Activity From Partners” tool also allows users to choose whether data that third parties share with Meta about their activities on other websites and apps can be used to show them personalized ads. *Id.* ¶ 12; *see also* Barrera Decl., Exs. F, G, H, I (collecting screenshots and articles regarding these tools).

B. Meta’s Restrictions On Use Of The Pixel Tool

The Meta Pixel tool is available to web developers across numerous industries, and each developer who configures the Pixel code on their website chooses what types of user activity to measure. Wooldridge Decl. ¶¶ 3–4. Meta does not want to receive health information, or any other sensitive data, from developers who use Pixel. *Id.* ¶ 5. Accordingly, Meta takes several measures designed to (1) prevent the transmission of such data and (2) block any such data that *is* transmitted.

First, Meta requires developers who choose to use the Pixel tool to warrant that they have the legal right to share any information they choose to send to Meta, and expressly prohibits developers from sending health-related or otherwise sensitive information. *Id.* ¶ 6. Those requirements are set forth in clear and direct terms. Before integrating the Pixel code on their website, developers must agree to the Business Tools Terms, described in detail above. Barrera Decl., Ex. D at 1–4. Developers must also agree to Meta’s Commercial Terms before using Meta for a business purpose; those terms similarly provide that developers cannot send Meta any “information that . . . includes health, financial, biometrics, or other categories of similarly sensitive information (including any information defined as

sensitive under applicable law).” Barrera Decl., Ex. E at 2; Wooldridge Decl. ¶ 6. Meta repeatedly reminds developers not to send this information, including during the “Pixel ID” creation process—a necessary step to install and use the Pixel—when developers are told not to send Meta sensitive user data, and are provided a link to Meta’s Business Help Center page about restricted data. Wooldridge Decl. ¶ 7.

Second, Meta has implemented a filtering mechanism to screen out potentially sensitive health data it detects that is sent in violation of these policies. *Id.* ¶ 8. Meta developed the filter to detect data sent through the Pixel that Meta categorizes as even *potentially* sensitive—including health data—and the filter prevents any such data it detects from being ingested into Meta’s ads ranking and optimization systems. *Id.* [REDACTED]

[REDACTED]. *Id.* When Meta’s systems filter out data detected as potentially sensitive, Meta sends notifications to the developer. *Id.* ¶ 9. These notifications warn that potential health data was detected and blocked and provide details about the affected data—including the URL where the events occurred, the location of the potentially violating information, steps the developer can take to address the issue, and an email address to contact with questions. *Id.*

C. Previous Litigation

In 2016, a group of plaintiffs represented by the same counsel as in this case sued Meta (then called Facebook) and several healthcare providers over Meta’s alleged collection of information about their browsing histories on the providers’ websites. The plaintiffs alleged that this collection took place when healthcare providers placed certain Meta code (such as the “Like” button) on their websites, which resulted in Meta obtaining the URLs of those webpages via cookies when users visited them. *See Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 948 (N.D. Cal. 2017). They further alleged that collecting information about their browsing activities on the healthcare sites—for example, a user’s visit to “pages containing information about treatment options for melanoma,” or a query for “search results related to the phrase ‘intestine transplant’”—revealed their “sensitive medical information,” and

1 that this communication did not comply with heightened consent standards established by HIPAA. *Id.*
 2 at 954–55. They brought claims against Meta and the healthcare providers under the Electronic
 3 Communications Privacy Act, the California Invasion of Privacy Act, the California constitution, and
 4 California contract and tort law. *Id.* at 949.

5 Judge Davila granted Meta’s motion to dismiss, holding that the plaintiffs had “consented to
 6 [Meta]’s tracking activity” by “agree[ing] to several [Meta] policies when they signed up for accounts”;
 7 these policies contained “broad disclosures . . . about how [Meta] tracks users to improve its ad
 8 targeting.” *Id.* at 953. The court rejected the plaintiffs’ argument that Meta’s disclosures were
 9 insufficient because they “d[id] not meet HIPAA’s heightened authorization requirements.” *Id.* at 954.
 10 The court dismissed with prejudice because, in light of the plaintiffs’ consent, “amendment would be
 11 futile.” *Id.* at 956. The Ninth Circuit affirmed. *Smith v. Facebook, Inc.*, 745 F. App’x 8 (9th Cir.
 12 2018). In light of its holding that consent barred all of the plaintiffs’ claims, the court did not reach
 13 Meta’s other arguments for dismissal. *Id.* at 9.

14 **D. Procedural History**

15 Plaintiffs are four Facebook users who logged into patient portals on healthcare providers’
 16 websites. Compl. ¶¶ 32–35. They allege that each of their healthcare providers—MedStar Health
 17 System, Rush University System for Health, and UK Healthcare, none of which is named as a
 18 defendant—installed the Meta Pixel on their patient portals. *See id.* ¶¶ 3–11. As a result, plaintiffs
 19 say, the providers sent Meta information about “when they register, log-in and logout of patient portals
 20 and set up appointments.” *Id.* ¶ 12; *see also, e.g., id.* ¶¶ 5, 7–8, 86, 122, 146 (recounting information
 21 allegedly sent by Meta’s Pixel). That information, plaintiffs allege, revealed their status as patients and
 22 is therefore subject to HIPAA’s heightened consent requirements because, plaintiffs say, “[p]atient
 23 status alone is protected by HIPAA.” *Id.* ¶ 44. Plaintiffs do *not* allege that they have ever used the
 24 tools Meta provides to disconnect off-Facebook activity from their accounts or to clear their history of
 25 third-party activity data. *See supra* at 6.

26 Plaintiffs sued in June 2022 and brought eight claims against Meta. Four challenge Meta’s
 27 receipt of information from healthcare providers that placed the Meta Pixel on their websites. *See id.*
 28 ¶¶ 131–38 (California privacy tort law), 139–55 (Electronic Communications Privacy Act), 156–65

(California Invasion of Privacy Act), 188–99 (trespass). Three more challenge Meta’s alleged failure to ensure healthcare providers who installed Meta’s Pixel were complying with HIPAA. *See id.* ¶¶ 108–23 (breach of contract), 124–30 (breach of the implied covenant of good faith and fair dealing), 166–73 (negligent misrepresentation). Plaintiffs also bring a claim for alleged violations of California’s Unfair Competition Law. *See id.* ¶¶ 174–87.

On August 25—more than two months after filing suit, and shortly after three similar cases had been filed—plaintiffs filed a motion for a preliminary injunction. Dkt. 46 (“Mot.”). The motion rests on plaintiffs’ claims under ECPA, CIPA, and California tort law. *Id.* at 1. It seeks an order broadly “enjoin[ing] Defendant Meta Platforms, Inc. (‘Meta’) from intercepting patient information and communications from HIPAA-covered entities through its use of the Meta Pixel” and “enjoin[ing] Meta from disseminating and/or using patient information and communications that it has intercepted from HIPAA-covered entities through its use of the Meta Pixel.” Dkt. 46-1 at 1.

This case is one of four consolidated cases currently before the Court, with three more inbound. *See* Dkt. 73; *Krackenberger v. Northwestern Memorial Hosp., et al.*, No. 1:22-cv-04203 (N.D. Ill.) (transferred October 6); *Smidga v. Meta Platforms, Inc., et al.*, No. 2:22-cv-01231-MPK (W.D. Pa.) (transferred October 5); *Naugle, et al. v. Meta Platforms, Inc., et al.*, No. 1:22-cv-00727-UA-JEP (M.D.N.C.) (agreed transfer motion forthcoming). The consolidation order provides that this Court will appoint lead counsel, who will “file a consolidated complaint” that “shall be the operative complaint in the consolidated action and shall supersede all complaints filed in any action consolidated herein.” Dkt. 73 ¶¶ 6, 10. The order also provides that Meta “shall not be required to respond to the complaint in any action consolidated into this action, other than the consolidated complaint.” *Id.* ¶ 5.

LEGAL STANDARD

“A preliminary injunction is an extraordinary remedy never awarded as of right.” *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 24 (2008). “A plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest.” *Id.* at 20. Where, as here, a party seeks a “mandatory injunction”—*i.e.*, one that requires “affirmative action,” rather than “maintaining the status quo”—the burden is “doubly

demanding” and preliminary relief is “particularly disfavored.” *Garcia v. Google, Inc.*, 786 F.3d 733, 740 (9th Cir. 2015) (en banc) (quotation marks and citation omitted). “The district court should deny such relief unless the facts and law *clearly favor* the moving party.” *Id.* (emphasis added). “In general, mandatory injunctions are not granted unless extreme or very serious damage will result and are not issued in doubtful cases or where the injury complained of is capable of compensation in damages.” *Marlyn Nutraceuticals, Inc. v. Mucos Pharma GmbH & Co.*, 571 F.3d 873, 879 (9th Cir. 2009) (quotation marks and citation omitted); *see also, e.g., Barrilleaux v. Mendocino Cnty.*, 2016 WL 4269328, at *1 (N.D. Cal. Aug. 15, 2016).

ARGUMENT

Plaintiffs want this Court to order Meta to stop receiving or using their “patient information and communications,” even though it is *third-party web developers* who choose whether to send that information to Meta and *plaintiffs themselves* who could disconnect off-Facebook activity from their accounts. Plaintiffs do not even try to propose an injunction tailored to the problem they identify, nor do they overcome the numerous fundamental factual and legal problems in their legal theories and claims for relief. Their motion comes nowhere close to justifying the extraordinary remedy they seek.

I. The Planned Consolidated Amended Complaint Moots Plaintiffs’ Motion.

“It is well-established in [the Ninth Circuit] that an amended complaint supersedes the original, the latter being treated thereafter as non-existent.” *Ramirez v. Cnty. of San Bernardino*, 806 F.3d 1002, 1008 (9th Cir. 2015). This Court has ordered that “[t]he consolidated complaint shall be the operative complaint in the consolidated action and shall supersede all complaints filed in any action consolidated herein,” and has made clear that Meta “shall not be required to respond to the complaint in any action consolidated into this action, other than the consolidated complaint.” Dkt. 73 ¶¶ 5–6. As a result of this order, the amended complaint filed in *John Doe* is no longer operative, and the preliminary injunction motion based on that complaint is moot. Numerous cases have held exactly that.⁴

⁴ *E.g., Garcia v. Mid-Atl. Military Family Communities LLC*, 2021 WL 1429474, at *3 (E.D. Va. Mar. 4, 2021); *Clay v. Wells Fargo Home Mortg., N.A.*, 2013 WL 1189712, at *2 (E.D. Cal. Mar. 21, 2013); Dkt. 63, *Techtronic Power Tools Tech. Ltd. v. Harbor Freight Tools USA, Inc.*, No. 8:20-cv-2004 (D.S.C. Oct. 21, 2020); Dkt. 20, *Geisert v. Brown*, No. 3:9-cv-670 (N.D. Tex. Mar. 22, 2010).

Notably, this rule applies regardless of whether plaintiffs expect the consolidated amended complaint to differ materially from the amended complaint filed in *John Doe*. A motion based on an inoperative pleading is moot even when the initial complaint and the amended complaint are “substantively the same.” *Falck N. Cal. Corp. v. Scott Griffith Collaborative Sols., LLC*, 25 F.4th 763, 764–66 (9th Cir. 2022) (holding initial complaint “is a legal nullity even if much like the operative complaint,” rejecting argument that court “could grant effective relief because [the initial complaint] is substantively the same as [the] amended complaint,” and dismissing as moot interlocutory appeal of denial of anti-SLAPP motion). The purpose of consolidation is to streamline litigation into a single case and avoid piecemeal litigation of motions tethered to superseded complaints.

II. Plaintiffs Cannot Meet Their Heavy Burden To Justify A Preliminary Injunction.

Plaintiffs’ motion also fails on the merits. They cannot show irreparable harm; neither the balance of equities nor the public interest tips in their favor; and they are not likely to succeed on the merits. Plaintiffs are not entitled to relief under any standard—much less the “doubly demanding” standard for a preliminary injunction that would require Meta to take affirmative action to change the status quo. *Garcia*, 786 F.3d at 740.

A. Plaintiffs Will Not Suffer Irreparable Harm Absent A Preliminary Injunction.

To justify a mandatory injunction, plaintiffs must show “extreme or very serious damage will result” without one. *Marlyn Nutraceuticals*, 571 F.3d at 879. For several reasons, they cannot do so.

1. Plaintiffs’ “long delay before seeking a preliminary injunction implies a lack of urgency and irreparable harm.” *Oakland Tribune, Inc. v. Chronicle Pub. Co.*, 762 F.2d 1374, 1377 (9th Cir. 1985); *see also, e.g., Garcia*, 786 F.3d at 746 (months of delay “undercut [plaintiff’s] claim of irreparable harm”). Plaintiffs waited more than two months to seek a preliminary injunction, and finally did so only after other plaintiffs’ counsel began filing related lawsuits.

2. Plaintiffs have “not shown a sufficient causal connection between irreparable harm” and Meta’s conduct. *Perfect 10, Inc. v. Google, Inc.*, 653 F.3d 976, 982 (9th Cir. 2011) (no preliminary injunction where plaintiff failed to connect alleged harm to “Google’s operation of its search engine”). The exact opposite is true. Plaintiffs say “the irreparable harm Meta has caused and will continue to

1 cause is the *interference with the patient Class’s right to confidential medical care and*
 2 *communications.*” Mot. at 19 (emphasis added). That theory runs straight into several fundamental
 3 factual problems.

4 First, plaintiffs can disconnect their off-Facebook activity from their accounts at any time,
 5 including on a website-by-website basis, but do not allege that they have done so. *See supra* at 6; *see*
 6 *also* Dkt. 49 at 11 n.3 (plaintiffs’ declaration acknowledging MedStar disclosure that users can
 7 “‘unlink’ their Facebook account from the MedStar website”). Injuries that are “avoidable” or “self-
 8 inflicted” are “not irreparable harm.” *Al Otro Lado v. Wolf*, 952 F.3d 999, 1008 (9th Cir. 2020); *see*
 9 *also, e.g., Adtrader, Inc. v. Google LLC*, 2018 WL 1876950, at *4 (N.D. Cal. Apr. 19, 2018) (no
 10 irreparable injury where plaintiffs were “free to opt out” of challenged dispute resolution agreement);
 11 *Brien v. J.P. Morgan Chase Bank, N.A.*, 2010 WL 11597807, at *2 (C.D. Cal. Nov. 24, 2010) (no
 12 irreparable injury where plaintiffs “can easily mitigate the alleged harm”). The fact that plaintiffs have
 13 not taken even this basic step is fatal to their request for extraordinary relief.

14 Second, plaintiffs have not shown their alleged harm is caused *by the defendant*. Meta already
 15 takes extensive measures to prevent third-party developers from sending it sensitive information.
 16 Plaintiffs are “confident” that “Meta is able to identify all web properties from which it is currently
 17 acquiring such patient information—and to immediately stop the data flow.” Mot. at 2. Plaintiffs may
 18 be confident, but they are wrong. It is third-party *web developers*, not Meta, who decide how to
 19 configure the code on their websites to send their chosen information to Meta, and it is not clear what
 20 plaintiffs’ injunction would have Meta do beyond what it already does: instruct developers not to send
 21 sensitive data; require them to agree to a contract warranting as much; attempt to filter out any
 22 potentially sensitive data developers nonetheless send; and notify developers when Meta detects
 23 potentially sensitive data, and instruct them to take steps to ensure they are not sending sensitive
 24 information. *See supra* at 6–7.

25 Plaintiffs’ own submission underscores that it is not *Meta’s* conduct at issue. John Doe—the
 26 only plaintiff who submitted a declaration in support of plaintiffs’ motion—concedes that it is the
 27 healthcare sites’ conduct, not Meta’s, that plaintiffs seek to change: He states that he “would like to be
 28 able to freely use the MedStar patient portal again *after MedStar removes its third-party tracking tools*,

including the Facebook Pixel.” Dkt. 47 ¶ 8 (emphasis added). That contemplates action by *MedStar*, not by Meta; if plaintiffs are concerned with how healthcare providers configure the Pixel tool on their own websites (in spite of Meta’s requirements and data filtering systems), then the proper parties to sue would be the providers themselves. *Cf. Hartmann v. Cal. Dep’t of Corr. & Rehab.*, 707 F.3d 1114, 1127 (9th Cir. 2013) (plaintiff challenging state policy must “name the official within the entity who can appropriately respond to injunctive relief”).⁵ Indeed, plaintiffs’ own declaration states that since the complaint in this case was filed, several healthcare providers have “recently removed the Meta Pixel” from their own websites. Dkt. 49 at 104.

B. The Balance Of Equities Does Not Tip In Plaintiffs’ Favor.

To assess the relative equities, the court “must balance the competing claims of injury and must consider the effect on each party of the granting or withholding of the requested relief.” *Amoco Prod. Co. v. Vill. of Gambell*, 480 U.S. 531, 542 (1987). Because plaintiffs acknowledge that they already have the ability to disconnect off-Facebook activity from their accounts, but have not chosen to take this basic step, any harm to them from withholding injunctive relief is minimal. *Cf. Envtl. Democracy Project v. Green Sage Mgmt., LLC*, 2022 WL 4596616, at *4 (N.D. Cal. Aug. 23, 2022) (“the balance of equities favors Plaintiff because Defendant’s alleged harms are self-inflicted”).

But the harm to Meta if this Court issues an injunction would be significant. Plaintiffs broadly demand that Meta stop receiving *all* “patient information and communications” from *all* “HIPAA-covered entities” using the Pixel tool, Dkt. 46-1 at 1, but they offer no solution that is tailored to the problem they identify—the receipt of *sensitive* information—beyond the steps Meta already takes to prevent the use and receipt of even potentially sensitive data. Imposing an injunction on Meta under these circumstances—where it is already making extensive efforts to prevent the receipt and use of

⁵ In an attorney declaration submitted along with their preliminary injunction motion, plaintiffs cited and attached state cases not involving Meta, in which individuals did exactly that: sued healthcare providers based on the information they allegedly shared with third parties. *See* Dkt. 48; *see also* Mot. at 15 (arguing that “deployment of the Meta Pixel on a medical provider website associated with a patient portal sets forth a viable claim *against the medical provider* for violation of state criminal laws”) (emphasis added). In fact, plaintiffs’ leading case expressly states that it “does not hinge on the relationship between the Plaintiff and Facebook.” *Doe v. Va. Mason Med. Ctr.*, 2020 WL 1983046, at *2 (Wash. Sup. Ct. Feb. 12, 2020).

1 potentially sensitive data, and plaintiffs have no suggestions for what more it could do—would be
2 decidedly inequitable.

3 Rule 65(d) recognizes the harm that may flow from such a vague injunction: a motion for
4 injunctive relief must “state its terms specifically” and “describe in reasonable detail . . . *the act or acts*
5 *restrained or required.*” Fed. R. Civ. P. 65(d); *see also, e.g., United States v. Holtzman*, 762 F.2d 720,
6 726 (9th Cir. 1985) (“Rule 65(d) requires the language of injunctions to be reasonably clear so that
7 ordinary persons will know precisely what action is proscribed.”). Plaintiffs make no serious attempt
8 to meet that requirement; they simply assert that their injunction “merely requires compliance” with
9 the law. Mot. at 20. For the reasons discussed below (at 15–24), that is incorrect; Meta’s existing
10 practices go *beyond* what the law requires. And in any event, plaintiffs’ conclusory assertion falls far
11 short of meeting their burden to identify the relative harms and demonstrate that the balance tips in
12 their favor.

13 C. A Preliminary Injunction Is Not In The Public Interest.

14 When “the impact of an injunction reaches beyond the parties,” courts must consider the
15 broader effects of any injunction and “may in the public interest withhold relief until a final
16 determination of the rights of the parties, though the postponement may be burdensome to the plaintiff.”
17 *Stormans, Inc. v. Selecky*, 586 F.3d 1109, 1139 (9th Cir. 2009); *see also, e.g., Bernhardt v. Los Angeles*
18 *Cnty.*, 339 F.3d 920, 931 (9th Cir. 2003) (“The public interest inquiry primarily addresses impact on
19 non-parties rather than parties.”). Again, plaintiffs are not clear about how their proposed injunction
20 would actually operate. Although their proposed order applies only to Meta, plaintiffs’ motion seeks
21 an injunction against not just Meta but also “all other persons acting in concert with it,” and as explained
22 above, John Doe’s declaration contemplates action by MedStar, not Meta. *Compare* Dkt. 46-1 at 1
23 (proposed order), *with* Mot. at 1, *and* Dkt. 47 ¶ 8 (declaration of John Doe). If plaintiffs seek an
24 injunction against Meta only, then it would be ineffective—because developers (not Meta) control the
25 code on their own websites and choose which information to send, and Meta *already* has measures in
26 place to prevent the receipt and use of sensitive information. *See supra* at 6–7. If plaintiffs seek an
27 injunction against every medical provider who uses the Meta Pixel, by contrast, then the burden on
28 non-parties would be sprawling and substantial. *See* Mot. at 2 (purporting to identify 660 non-party

1 medical providers). The public interest thus weighs strongly against injunctive relief that, to be
2 effective, would operate against (at least) many hundreds of non-parties.

3 Plaintiffs do not address this burden on non-parties. Instead, they simply extol the importance
4 of privacy in general and assert hyperbolically that “Meta is creating a turn-key solution for
5 totalitarianism.” Mot. at 21–22. That rhetoric is misplaced. This case is not a referendum on privacy
6 in general, nor does it have anything to do with making “governmental actors [] immune from the same
7 or similar conduct.” *Id.* at 22. It is, rather, about the ways in which website developers—with full
8 disclosure and user consent, and subject to user controls—use a common Internet tool to facilitate
9 online advertising. Plaintiffs cannot rely on vague and overwrought abstractions as a substitute for the
10 concrete showing necessary to justify a preliminary injunction.

11 **D. Plaintiffs Are Unlikely To Succeed On The Merits.**

12 To justify a preliminary injunction that requires affirmative action by Meta (or other parties,
13 like the healthcare companies who would be affected by plaintiffs’ proposed relief), plaintiffs “must
14 establish that the law and facts *clearly favor* [their] position, not simply that [they are] likely to
15 succeed.” *Garcia*, 786 F.3d at 740. Plaintiffs cannot meet even the more lenient standard, both because
16 the overarching issue of consent bars all of their claims and for reasons specific to each claim.

17 **1. Consent bars all of plaintiffs’ claims.**

18 **(i) Plaintiffs consented to Meta’s collection of information when 19 they signed up for a Facebook account.**

20 Plaintiffs base their preliminary injunction motion on their claims brought under ECPA, CIPA,
21 and California privacy tort law. *See* Mot. at 1. The absence of consent is an express or implied element
22 of each of these claims.⁶ And while “[t]here may be subtle differences” among the consent doctrines
23 applicable to each claim, “the question under [each] is essentially the same: Would a reasonable user

24
25 ⁶ Under ECPA, “[i]t shall not be unlawful . . . for a person not acting under color of law to intercept a
26 wire, oral, or electronic communication where . . . one of the parties to the communication has given
27 prior consent to such interception.” 18 U.S.C. § 2511(2)(d). Under CIPA, plaintiffs must show a
28 defendant intercepted covered information “without the consent of all parties” to the communication.
Cal. Penal Code §§ 631(a), 632(a). For a California privacy tort claim, the general “maxim of the law
‘*violenti non fit injuria*’ (no wrong is done to one who consents) applies as well to the invasion of
privacy tort.” *Hill v. Nat’l Coll. Athletic Ass’n*, 865 P.2d 633, 648 (Cal. 1994); *see also* Restatement
(Second) of Torts § 892A (1979) (“One who effectively consents to conduct of another intended to
invade his interests cannot recover in an action of tort for the conduct.”).

1 who viewed [Meta’s] disclosures have understood that [Meta] was collecting [the information at
 2 issue]?” *Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1212 (N.D. Cal. 2014) (discussing ECPA
 3 and Stored Communications Act claims); *see also Smith*, 745 F. App’x at 8. Plaintiffs’ claims all fail
 4 under this standard, because Meta disclosed the use of the Pixel tool in policies that every Facebook
 5 user agrees to when they sign up for an account.

6 Plaintiffs admit they are “legally deemed to have agreed” to three of Meta’s relevant policies—
 7 its Terms of Service, Data Policy, and Cookies Policy—and that those policies contractually bind them.
 8 Compl. ¶ 49. The Data Policy informs users that “[a]dvertisers, app developers, and publishers can
 9 send [Meta] information through Meta Business Tools they use, including . . . the Meta pixel,” with a
 10 hyperlink from “Meta pixel” to a page containing additional information. Barrera Decl., Ex. B at 4.
 11 The Data Policy further explains that “[t]hese partners provide information about your activities off of
 12 our Products . . . whether or not you have an account or are logged into our Products,” and includes
 13 examples: “information about your device, websites you visit, purchases you make, the ads you see,
 14 and how you use their services.” *Id.* at 4–5. The Data Policy provides additional examples and
 15 explanations, and invites users to “learn more about how [Meta] use[s] cookies in connection with Meta
 16 Business Tools” by reviewing the Cookies Policy, *id.* at 5—which itself explains that Meta could
 17 receive “information about your use of other websites and apps” and use that information to “show
 18 ads,” as well as a description of the specific cookie that enables Pixel, Barrera Decl., Ex. C at 1–2.
 19 These disclosures (and others) amply communicated to users that Meta collected information about
 20 their activities on third-party websites. *Cf. Smith*, 745 F. App’x at 8.

21 **(ii) Plaintiffs’ attempts to circumvent *Smith* fail.**

22 In *Smith*, the Ninth Circuit affirmed the district court’s holding that, as a matter of law, the
 23 plaintiffs had “consented to Facebook’s data tracking and collection practices” in light of the
 24 “numerous disclosures related to information collection on third-party websites” in Facebook’s
 25 policies. 745 F. App’x at 8. “A reasonable person viewing those disclosures would understand that
 26 Facebook maintains the practices of (a) collecting its users’ data from third-party sites and (b) later
 27 using the data for advertising purposes,” the court held, and “[k]nowing authorization of the practice
 28 constitutes Plaintiffs’ consent.” *Id.* at 8–9. The court expressly rejected the plaintiffs’ argument that

1 they had provided only “general consent” and “did not consent to the collection of health-related data
2 due to its ‘qualitatively different’ and ‘sensitive’ nature.” *Id.* at 9.⁷

3 So too here: Plaintiffs consented to Meta’s collection of information about their activity on
4 third-party websites, and that consent bars each of their claims. As in *Smith*, a reasonable person
5 viewing Meta’s disclosures—including disclosures specifically about Pixel and Meta’s receipt of
6 “information about your activities off of our Products,” such as the “websites you visit” and “how you
7 use their services,” Barrera Decl., Ex. B at 4—would understand that Meta collects information about
8 user activities on third-party websites and uses that information for advertising purposes. *See also*
9 *Perkins*, 53 F. Supp. 3d at 1212. And as in *Smith*, plaintiffs’ “[k]nowing authorization of the practice
10 constitutes Plaintiffs’ consent.” 745 F. App’x at 9. Indeed, the case for consent here is even stronger
11 than in *Smith*, because plaintiffs could disconnect off-Facebook activity from their accounts at any time
12 (including on a website-by-website basis, which would allow plaintiffs to disconnect from their
13 respective healthcare providers’ sites). *See supra* at 6. Plaintiffs’ claims therefore fail.

14 Trying to circumvent that result, plaintiffs claim there are “four key differences between this
15 case and *Smith*.” Mot. at 7. None of those “key differences” changes the analysis.

16 ***HIPAA does not replace Smith’s standard for consent.*** Plaintiffs’ first three attempts to
17 distinguish *Smith* all seek to invoke HIPAA’s heightened consent standard. They say (1) “*Smith* was
18 not limited to patients,” (2) “the ‘medical’ websites at issue in *Smith* were not limited to HIPAA-
19 covered entities,” and (3) “*Smith* had not distinguished the data at issue as *patient*-data.” Mot. at 7.
20 Those differences, plaintiffs argue, justify uprooting *Smith*’s “reasonable user” standard for consent
21 and supplanting it with HIPAA’s complex regulatory scheme. HIPAA’s implementing regulations
22 provide that certain entities, for certain uses and disclosures of certain health information, must obtain
23 a “valid authorization” meeting a detailed list of requirements—*e.g.*, descriptions of the information to
24

25 ⁷ Here again, plaintiffs say their consent is ineffective because “consent must be . . . to the particular
26 conduct or substantially the same conduct.” Mot. at 8 (quoting *Tsao v. Desert Palace, Inc.*, 698 F.3d
27 1128, 1149 (9th Cir. 2012)). But Meta’s policies broadly described third parties’ ability to measure
28 activity on their websites using the Meta Pixel, and “[a] contractual term is not ambiguous just because
it is broad.” *F.B.T. Prods., LLC v. Aftermath Records*, 621 F.3d 958, 964 (9th Cir. 2010). Plaintiffs’
only response is to recite the Data Policy’s statement that Meta requires developers to have lawful
rights to send information to Meta, *see* Mot. at 8–9, but for the reasons below, that does nothing to
vitate plaintiffs’ consent. *See infra* at 18–20.

1 be used or disclosed, the parties who may make and receive the disclosure, the purpose of the
 2 disclosure, information about the individual’s right to revoke authorization, and more. *See* 45 C.F.R.
 3 § 164.508(c); *see generally id.* §§ 164.502, 164.508. That detailed scheme differs from the standard
 4 for consent applicable to plaintiffs’ claims: whether “a reasonable user who viewed [Meta’s]
 5 disclosures [would] have understood that [Meta] was collecting” the information at issue. *Perkins*, 53
 6 F. Supp. 3d at 1212; *see also Smith*, 745 F. App’x at 8.

7 Plaintiffs’ bid to import HIPAA’s consent standard into this case fails as a matter of law,
 8 principally because HIPAA does not provide a private right of action. *Webb v. Smart Document Sols.,*
 9 *LLC*, 499 F.3d 1078, 1082 (9th Cir. 2007); 65 Fed. Reg. 82601 (Dec. 28, 2000). Litigants cannot plead
 10 around that problem by channeling substantive standards from one claim (which they cannot bring)
 11 through another, different claim. *Cf. Astra USA, Inc. v. Santa Clara Cnty.*, 563 U.S. 110, 114 (2011)
 12 (where a statute does not provide a private right of action, “it would make scant sense to allow
 13 [plaintiffs] to sue on a form contract implementing the statute”). A contrary conclusion would render
 14 meaningless congressional decisions to withhold a private right of action—and the extensive body of
 15 law addressing that question statute-by-statute—because if “every statute that specified a standard of
 16 care [were] automatically enforceable by tort suits for damages,” then “every statute in effect would
 17 create an implied private right of action.” *Cuyler v. United States*, 362 F.3d 949, 952 (7th Cir. 2004).
 18 That “clearly is not the law.” *Id.* And it is why courts have refused attempts by plaintiffs to effectively
 19 bring claims they cannot bring directly through the backdoor of other causes of action. *See, e.g., Miller*
 20 *v. Elam*, 2011 WL 1549398, at *4 (E.D. Cal. Apr. 21, 2011) (“Because there is no private right of
 21 action under HIPAA, plaintiff’s HIPAA claim is not cognizable under 42 U.S.C. § 1983.”); *Zhang v.*
 22 *Superior Court*, 304 P.3d 163, 177 (Cal. 2013) (where there is no private right of action, “a litigant
 23 may not rely on the proscriptions of [that statute] as the basis for a UCL claim”).

24 ***Plaintiffs’ contract claims do not vitiate their consent.*** Plaintiffs next contend that “Meta’s
 25 current contract and promises to users are different than they were in *Smith*,” Mot. at 7—specifically,
 26 the Data Policy was updated in 2018 to state that Meta “require[s]” third parties who send information
 27 through Pixel to “have lawful rights to collect, use and share your data before providing any data to
 28

us.” Barrera Decl., Ex. B at 5. Plaintiffs say that because Meta did not adequately “enforce its promise,” their consent was based on a “mistake” and is therefore invalid. Mot. at 9.

Every part of that argument is wrong. *First*, there is no “mistake”: Meta *does* require third parties to have lawful rights to share user data. Meta’s publicly available Business Tools Terms—which any third party who wishes to use Pixel must agree to—requires web developers to “represent and warrant that you (and any data provider that you may use) have all of the necessary rights and permissions and a lawful basis (in compliance with all applicable laws, regulations and industry guidelines) for the disclosure and use of Business Tool Data.” Barrera Decl., Ex. D at 1; *see also id.* at 3 (requiring web developers to provide their users with “robust and sufficiently prominent notice” about data collection). That is precisely the requirement contemplated in Meta’s Data Policy. Plaintiffs do not—because they cannot—dispute this. Instead, they assert Meta breached its promise by failing to make “any effort to enforce its promise” *beyond* the “provision in its form contract with developers.” Mot. at 9. But Meta’s policies did not promise any particular enforcement process. *See, e.g., Illinois v. Facebook*, No. 2018 CH 3868, at *11 (Ill. Cir. Ct. Mar. 8, 2021) (“Facebook’s relevant policies only indicate the enforcement available to it and Facebook makes no guarantee as to how it will proceed”). Plaintiffs have failed to show any breach of any promise Meta actually made. *Cf. Lee v. Canada Goose US, Inc.*, 2021 WL 2665955, at *6 (S.D.N.Y. June 29, 2021) (statements about company practices are not inaccurate simply because plaintiffs allege they are “insufficient and unsatisfactory”).

Second, even if Meta had promised some additional level of “enforcement,” there still would not be any “mistake” because Meta already engages in extensive efforts to avoid receiving sensitive information, including potentially sensitive health-related information. *See supra* at 6–7. Plaintiffs say that “to [their] knowledge, the only evidence that Meta makes any effort to enforce its promise is that it includes a provision in its form contract with developers stating that the developer asserts it has permission to send Meta data.” Mot. at 9. That is inaccurate. In addition to requiring web developers to warrant that they have the legal right to share any information they send to Meta, Meta expressly instructs them not to send any “health” information. Barrera Decl., Ex. D at 2. If they nevertheless do so, Meta has systems in place to filter and screen out information sent through Pixel that it detects and categorizes as potentially sensitive, including health data. Wooldridge Decl. ¶ 8. When potentially

sensitive information is detected, Meta prevents it from being ingested into Meta’s ads ranking and optimization systems, and Meta sends notifications to the developer warning it to ensure it is not using Meta’s Pixel to send sensitive data (along with instructions for doing so). *Id.* ¶ 9.

Third, even if plaintiffs could show a breach of the Data Policy, it would not vitiate their consent. Plaintiffs provided consent in three separate policies (the Terms of Service, Data Policy, and Cookies Policy)—each of which they allege is legally binding, each of which disclosed the practices at issue here, and none of which conditioned consent on any particular level of enforcement of any particular pledge made by Meta in those policies. *See* Compl. ¶ 49; *see supra* at 3–5. Those policies described the broad nature of the information Meta could receive from third parties, and a “contractual term is not ambiguous just because it is broad.” *F.B.T. Prods.*, 621 F.3d at 964. Even assuming Meta should have put *additional* enforcement mechanisms in place, plaintiffs were clearly informed that third parties had the ability to send Meta information about users’ activity on their websites.

2. Each of plaintiffs’ claims also fails for multiple other reasons.

(i) Plaintiffs’ ECPA claim is not likely to succeed.

ECPA is a one-party consent statute: there is no liability “where *one* of the parties to the communication has given prior consent,” unless “such communication is intercepted for the purpose of committing any criminal or tortious act.” 18 U.S.C. § 2511(2)(d) (emphasis added). Even assuming *plaintiffs* did not consent to sharing information with Meta, the healthcare providers who configured Pixel on their own websites clearly did, and the purpose for collecting the information—advertising—is not itself criminal or tortious. *See, e.g., Rodriguez v. Google LLC*, 2021 WL 2026726, at *6 n.8 (N.D. Cal. May 21, 2021); *In re Google Inc. Gmail Litig.*, 2014 WL 1102660, at *18 n.13 (N.D. Cal. Mar. 18, 2014); *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 518–19 (S.D.N.Y. 2001). That alone is enough to defeat plaintiffs’ ECPA claim.⁸

⁸ Plaintiffs make a conclusory assertion that Meta has a criminal or tortious purpose and simply list a number of allegedly violated laws, but this argument confuses Meta’s *receipt* of information with the *purpose* to which that information is allegedly put. *See Sussman v. Am. Broad. Cos., Inc.*, 186 F.3d 1200, 1202 (9th Cir. 1999) (“Under section 2511, the focus is not upon whether the interception itself violated another law; it is upon whether the purpose for the interception—its intended use—was criminal or tortious.” (quotation marks and citation omitted)).

Nor can plaintiffs show that all of the online activities healthcare providers allegedly measure qualify as “content,” as ECPA requires. *See* 18 U.S.C. § 2511. ECPA defines “contents” to include “any information concerning the substance, purport, or meaning of [a] communication.” 18 U.S.C. § 2510(8). Here, plaintiffs allege that the Meta Pixel measures their *activity* on patient portals and collects certain identifying information, including “the names of buttons they click on the website as well as their associated URLs” and “detailed URL information for the webpage the patient visited immediately preceding logging into the portal.” Mot. at 11–12. But not all activities that web developers choose to measure will reveal any “communication itself.” *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1107 (9th Cir. 2014). Plaintiffs also say this information can “reveal the patient’s HIPAA-protected patient status by way of the fact that they are a registered portal user.” Mot. at 12. But even if Meta can *infer* patient status from the activity information it obtains, that would not qualify as “content.” *See In re Zynga*, 750 F.3d at 1107 (deeming irrelevant what “an enterprising advertiser could uncover” using a referer header).

(ii) Plaintiffs’ CIPA claim is not likely to succeed.

Plaintiffs’ CIPA claim likewise fails. Plaintiffs allege that Meta violated two provisions of CIPA: Section 631(a) (the wiretapping provision) and Section 632(a) (the recording provision).

Section 631(a). Section 631(a), like ECPA, applies only to “the contents or meaning of any message, report, or communication.” Cal. Penal Code § 631(a); *see also Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020) (the “analysis for a violation of CIPA is the same as that under the federal [ECPA]”) (citation omitted). For the reasons above, plaintiffs cannot show that all of the activities healthcare providers choose to measure on their websites would qualify as “content.” *See supra* at 21.

Section 632(a). Section 632(a) applies only to eavesdropping or recording of “a *confidential* communication,” Cal. Penal Code § 632(a) (emphasis added), and “in California, courts have developed a presumption that Internet communications do not reasonably give rise to that expectation.” *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330, at *3 (N.D. Cal. Oct. 23, 2019) (collecting cases and holding that “browsing activity and form field entries” are not “confidential”); *see also, e.g., Cline v. Reetz-Laiolo*, 329 F. Supp. 3d 1000, 1051–52 (N.D. Cal. 2018) (emails not “confidential” despite

containing “private medical and financial information”) (Orrick, J.); *People v. Nakai*, 183 Cal. App. 4th 499, 517–18 (Cal. Ct. App. 2010) (instant messages, including sexually explicit photos, not “confidential communication,” despite sender’s “desire[] [for] the communication to be confidential”). That is particularly true here, where Meta’s policies informed users that their information could be collected on third-party websites. *Compare Nakai*, 183 Cal. App. 4th at 518 (pointing to disclosures in Yahoo!’s privacy policy as one reason instant messages were not “confidential”), *with Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1074 (N.D. Cal. 2021) (distinguishing *Nakai* where user was in “private browsing mode” and “Google’s policies did not indicate that data would be collected from users in private browsing mode”).

(iii) Plaintiffs’ California privacy tort claim is not likely to succeed.

To prevail on a claim for intrusion upon seclusion, plaintiffs must show that “(1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive.” *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020); *see also Hernandez v. Hillsides, Inc.*, 211 P.3d 1063, 1072 (Cal. 2009) (discussing elements for “common law tort of intrusion”); *Hill*, 865 P.2d at 657 (similar elements for “constitutional right to privacy”). They cannot meet either requirement.

The first—a reasonable expectation of privacy—is similar to the analysis of whether a communication is “confidential” under CIPA. *See In re Google Inc.*, 2013 WL 5423918, at *22 (“confidential communication” is one that plaintiff “had an objectively reasonable expectation was not being recorded”) (citation omitted). For the same reasons that their communications were not “confidential” under CIPA, *see supra* at 21–22, plaintiffs cannot show they had a reasonable expectation of privacy in them—a conclusion that is bolstered by Meta’s robust disclosures, because “notice, combined with [a plaintiff’s] written consent to the policy, defeats his claim that he had a reasonable expectation of privacy.” *TBG Ins. Servs. Corp. v. Superior Court*, 96 Cal. App. 4th 443, 452 (Cal. Ct. App. 2002).

Nor have plaintiffs shown that any intrusion was “highly offensive,” which contemplates “an exceptional kind of prying into another’s private affairs” such as “taking the photograph of a woman in the hospital with a rare disease that arouses public curiosity over her objection” or “using a telescope

1 to look into someone’s upstairs bedroom window for two weeks and taking intimate pictures with a
 2 telescopic lens.” *Med. Lab. Mgmt. Consultants v. Am. Broadcasting Cos.*, 306 F.3d 806, 819 (9th Cir.
 3 2002) (quotation marks omitted; citing Restatement (Second) of Torts § 652B). The allegations here—
 4 using consented-to online activity as a basis for improving online services—do not even approach that
 5 level of offensive intrusion. *Cf. Fogelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (Cal. Ct.
 6 App. 2011) (“obtaining plaintiff’s address without his knowledge or permission, and using it to mail
 7 him coupons and other advertisements,” was “not an egregious breach of social norms”).

8 To the contrary, “[c]ourts in this district have consistently refused to characterize the disclosure
 9 of common, basic digital information to third parties as serious or egregious violations of social norms.”
 10 *In re Google, Inc. Privacy Policy Litig.*, 58 F. Supp. 3d 968, 985 (N.D. Cal. 2014) (rejecting California
 11 constitutional claim based on disclosure of “personal identifying information, browsing habits, search
 12 queries, responsiveness to ads, demographic information, declared preferences and other information,”
 13 including “the contents of Gmail communications,” *id.* at 973); *see also, e.g., Hammerling v. Google*
 14 *LLC*, 2022 WL 2812188, at *12 (N.D. Cal. July 18, 2022) (collecting cases, rejecting claim based on
 15 collection of information from “fertility tracker app,” and noting that “[e]ven disclosure of highly
 16 personal information such as social security numbers is not ‘highly offensive’”); *McCoy v. Alphabet,*
 17 *Inc.*, 2021 WL 405816, at *7–8 (N.D. Cal. Feb. 2, 2021) (noting “the high bar in this district”). In the
 18 medical context, successful privacy claims have involved much more egregious circumstances: for
 19 example, in-person camera crews recording a person’s medical treatment immediately after a traumatic
 20 event and broadcasting it in a documentary or the nightly news,⁹ or using health records to
 21 “intimidate[], embarrass[] and humiliate[]” a victim of sexual battery.¹⁰ Again, the conduct alleged in
 22 this case is worlds away, and the improved online services related to the information Meta obtains lack
 23 the potential for public humiliation present in successful privacy cases.

24 The Ninth Circuit’s decision in *In re Facebook, Inc. Internet Tracking Litigation* is the
 25 exception that proves the rule. There, the court framed its reasonable-expectation-of-privacy analysis

26 _____
 27 ⁹ *See, e.g., Schulman v. Grp. W Prods., Inc.*, 955 P.2d 469, 474–75, 497 (Cal. 1998); *Miller v. Nat’l*
 28 *Broadcasting Co.*, 187 Cal. App. 3d 1463, 1469, 1483–84 (Cal. Ct. App. 1986).

¹⁰ *Susan S. v. Israels*, 55 Cal. App. 4th 1290, 1299 (Cal. Ct. App. 1997).

as asking “whether a user would reasonably expect that Facebook would have access to the user’s individual data *after the user logged out of the application*,” and it answered no because “Facebook’s privacy disclosures at the time allegedly failed to acknowledge its tracking of logged-out users, suggesting that users’ information would not be tracked.” 956 F.3d at 602 (emphasis added); *see also id.* (“Facebook set an expectation that logged-out user data would not be collected, but then collected it anyway.”). Plaintiffs’ claim is not based on logged-out tracking, nor could it be: the Data Policy discloses that Meta receives “information about your activities off of our Products . . . *whether or not you have an account or are logged into our Products*.” Barrera Decl., Ex. B at 4–5 (emphasis added). Similarly, the court concluded the plaintiffs in *In re Facebook* had “identified sufficient facts to survive a motion to dismiss” on the “highly offensive” prong in light of their “allegations of surreptitious data collection when individuals were not using Facebook.” 956 F.3d at 606. By contrast, where a policy is not “blatantly deceitful” about the information a company collects, courts have rejected claims that an alleged privacy intrusion was “highly offensive.” *See Hammerling*, 2022 WL 2812188, at *12 (distinguishing *In re Facebook* where policy was merely “ambiguous,” not “blatantly deceitful”).

III. Plaintiffs’ Requested Relief Is Impermissibly Overbroad.

Finally, even if preliminary relief were appropriate, the scope of the relief plaintiffs request here is wildly overbroad. “[A]n injunction must be narrowly tailored to affect only those persons over which [the court] has power, and to remedy only the specific harms shown by the plaintiffs, rather than to enjoin all possible breaches of the law.” *Price v. City of Stockton*, 390 F.3d 1105, 1117 (9th Cir. 2004) (quotation marks and citation omitted). The relief plaintiffs ask for runs afoul of that requirement for at least two reasons.

First, “in the absence of class certification, the preliminary injunction may properly cover only the named plaintiffs.” *Nat’l Ctr. for Immigrants Rights, Inc. v. I.N.S.*, 743 F.2d 1365, 1371 (9th Cir. 1984); *see also, e.g., California v. Azar*, 911 F.3d 558, 582–83 (9th Cir. 2018) (rule that scope of relief must be limited to parties before the court “applies with special force where there is no class certification”); *Easyriders Freedom F.I.G.H.T. v. Hannigan*, 92 F.3d 1486, 1501 (9th Cir. 1996) (“injunctive relief generally should be limited to apply only to named plaintiffs where there is no class certification”). There are four named plaintiffs in this action, and collectively they allege that they

1 used three medical providers’ patient portals: MedStar (John Doe, Jane Doe I), Rush (Jane Doe II), and
 2 UKH (John Doe II). Compl. ¶¶ 32–35. Only one of the named plaintiffs (John Doe) has submitted a
 3 declaration to provide any factual support. *See* Dkt. 47. Yet plaintiffs’ proposed order encompasses
 4 all “HIPAA-covered entities” that use Pixel, and they identify “more than 660 HIPAA-covered
 5 entities” as to which they seek relief. Mot. at 2. That is plainly overbroad. Moreover, on the merits,
 6 those entities will necessarily differ in how they use Pixel, what information they share, what
 7 disclosures they provide and consent they obtain from users, and any number of other relevant issues;
 8 plaintiffs’ proposed order accounts for none of those differences.

9 *Second*, in addition to sweeping in all “HIPAA-covered entities,” plaintiffs’ proposed order
 10 would apply to all “patient information and communications” from those entities. Dkt. 46-1 at 1. But
 11 not all “patient information and communications” are HIPAA-protected—and plaintiffs’ entire theory
 12 of the case hinges on their (incorrect) assertion that HIPAA provides the standard for consent. Nor are
 13 all “patient information and communications” necessarily “content” under ECPA or CIPA, or the sort
 14 of information that would make out a privacy tort. *See supra* at 21–24. The scope of plaintiffs’
 15 requested injunction is thus entirely untethered to the claims and legal theories they advance. *See*
 16 *NRDC v. Winter*, 508 F.3d 885, 886 (9th Cir. 2007) (“injunctive relief must be tailored to remedy the
 17 specific harm alleged”).

18 CONCLUSION

19 Plaintiffs’ motion should be dismissed as moot. If the Court does not dismiss it as moot, then
 20 the motion should be denied.

21
 22 DATED: October 17, 2022

GIBSON, DUNN & CRUTCHER LLP

23
 24 By: /s/ Lauren R. Goldman
 25 Lauren R. Goldman
 26
 27
 28

GIBSON, DUNN & CRUTCHER LLP
 LAUREN R. GOLDMAN (*pro hac vice*)
 lgoldman@gibsondunn.com
 200 Park Avenue
 New York, NY 10166
 Telephone: (212) 351-4000
 Facsimile: (212) 351-4035

ELIZABETH K. MCCLOSKEY (SBN 268184)
 emccloskey@gibsondunn.com
 ABIGAIL A. BARRERA (SBN 301746)
 abarrera@gibsondunn.com
 555 Mission Street, Suite 3000
 San Francisco, CA 94105
 Telephone: (415) 393-8200
 Facsimile: (415) 393-8306

TRENTON J. VAN OSS (*pro hac vice*)
 tvanoss@gibsondunn.com
 1050 Connecticut Avenue, N.W.
 Washington, DC 20036-5306
 Telephone: (202) 955-8500
 Facsimile: (202) 467-0539

*Attorneys for Defendant Meta Platforms, Inc.
 (formerly known as Facebook, Inc.)*

COOLEY LLP
 MICHAEL G. RHODES (SBN 116127)
 rhodesmg@cooley.com
 KYLE C. WONG (SBN 224021)
 kwong@cooley.com
 CAMERON J. CLARK (SBN 313039)
 cclark@cooley.com
 CAROLINE A. LEBEL (SBN 340067)
 clebel@cooley.com
 3 Embarcadero Center, 20th Floor
 San Francisco, CA 94111-4004
 Telephone: (415) 693-2000
 Facsimile: (415) 693-2222

UNITED STATES DISTRICT COURT
 NORTHERN DISTRICT OF CALIFORNIA
 SAN FRANCISCO DIVISION

IN RE META PIXEL HEALTHCARE
 LITIGATION

This Document Relates To:

Case No. 3:22-cv-3580-WHO (Doe)

Case No. 3:22-cv-3580-WHO

PUTATIVE CLASS ACTION

**DECLARATION OF TOBIAS
 WOOLDRIDGE IN SUPPORT OF
 DEFENDANT META PLATFORMS, INC.'S
 OPPOSITION TO PLAINTIFFS' MOTION
 FOR PRELIMINARY INJUNCTION**

*[Declaration of Abigail Barrera and [Proposed]
 Order filed concurrently herewith]*

Action Filed: June 17, 2022

Honorable Judge William H. Orrick

1 I, Tobias Wooldridge, hereby declare and state:

2 1. I am a software engineer at Meta. I offer this declaration in support of Meta's
3 Opposition to Plaintiff's Motion for Preliminary Injunction. The following facts are based on my own
4 personal knowledge, unless otherwise indicated, and, if called and sworn as a witness, I could and
5 would testify competently to them.

6 **My Background And Work At Meta**

7 2. I have worked at Meta as a software engineer since February 2015. I am a senior
8 engineer on the Signals team, which bears primary responsibility for maintaining and updating the
9 Meta Pixel code. My team is also responsible for maintaining and implementing Meta's systems that
10 detect and filter potentially sensitive data being sent by third-party developers to Meta via the Meta
11 Pixel, among other Business Tools. I have worked on the Signals team since April 2017.

12 **Meta Prohibits Developers From Sending Health Information Through Its Pixel Tool**

13 3. Meta's Pixel is a free, publicly available piece of code that third-party website
14 developers can choose to install and use on their websites to measure certain actions taken on their own
15 websites. Meta's Pixel is available to and used by website developers across industries. Other
16 companies offer their own pixel tools.

17 4. Specifically, when someone takes an action a developer chooses to track on their
18 website (like subscribing to email updates), the Meta Pixel is triggered and sends Meta certain data,
19 called an "Event." Meta attempts to match the Events it receives to Meta users (Meta cannot match
20 non-Meta users). The developer can then create "Custom Audiences" based on Events and can target
21 ads on Facebook, Instagram, and publishers within Meta's Audience Network to Meta users who have
22 taken certain actions on their own website. Meta can also provide the developer with de-identified,
23 aggregated reporting that helps the developer better understand the impact of its ads by measuring what
24 happens when people see them. The identity of matched Meta users is never revealed to the developer
25 or to any advertiser.

26 5. Meta does not want or permit developers to transmit sensitive information, including
27 health information, to it through the Pixel tool. Meta takes numerous measures to prevent the
28 transmission and receipt of that information.

1 6. First, Meta requires all developers to agree to its Business Tools Terms before they
2 can obtain a Pixel ID and utilize Meta Pixel code in a website. The Business Tools Terms expressly
3 prohibit developers from sending Meta health or otherwise sensitive information (including any
4 information defined as sensitive under applicable law) and require developers to warrant that they have
5 the legal right to share any information they choose to share with Meta. Developers must also accept
6 Meta's Commercial Terms before using Meta for a business purpose, which similarly prohibit sending
7 Meta health or otherwise sensitive information.

8 7. Second, during the Meta Pixel ID creation process—a necessary step to install and use
9 the Meta Pixel—Meta reminds developers not to send Meta sensitive user data, linking to the Business
10 Tools Terms and to Meta's Business Help Center content about restricted data ("About Restricted Meta
11 Business Tools Data"). Attached as **Exhibit 1** is a true and correct copy of the article entitled "About
12 Restricted Meta Business Tools Data," downloaded from the Meta Business Help Center on October
13 13, 2022. Meta has published several additional Business Help Center articles that explain and give
14 examples of the kinds of information (including health information) that developers should not send to
15 Meta, provide steps developers can take to avoid sending such information, and describe how to address
16 instances in which sensitive information may have been sent.

17 8. Third, in addition to requiring developers to agree not to send Meta any information
18 they do not have the legal right to share, Meta developed and implemented a filtering mechanism to
19 screen out potentially sensitive data it detects. Meta developed the filter to detect data sent through the
20 Pixel (as well as other Business Tools) that it categorizes as potentially sensitive data, including health
21 data, and the filter prevents that detected data from being ingested into Meta's ads ranking and
22 optimization systems. [REDACTED]

23 [REDACTED]
24 [REDACTED]
25 [REDACTED]
26 [REDACTED]
27 9. When Meta's systems detect and filter out data they categorize as potentially sensitive,
28 Meta sends notifications to the developer (1) via email and (2) in two locations in Meta's developer

1 dashboard, Events Manager. These notifications inform the developer that Meta detected and blocked
2 data that may not comply with Meta's terms; confirm that the removal may affect ad performance; and
3 provide details about the affected data, including the URL where the events occurred, the location (but
4 not the contents) of the potentially violating information, steps the developer can take to address the
5 issue, and an email address to contact with questions.

6 **Meta Users Consent To Meta's Use Of Pixel Data And Can Control And Disconnect Their Off-**
7 **Facebook Activity**

8 10. Meta discloses to users that it receives data from third parties, including data sent via
9 the Pixel tool, and provides several ways for its users to review and control Meta's use of that data.
10 The Data Policy, to which all users of Meta services must agree, explains that Meta may receive
11 information about users' activities off the Meta services, including from developers that use the Meta
12 Business Tools, including the Meta Pixel. The Data Policy also discloses how Meta uses such data,
13 including by providing measurement, analytics, and other business services. Meta users also must
14 agree to the Terms of Service and Cookies Policy, which disclose that their personal data can be used
15 to provide targeted ads.

16 11. Meta also enables its users to review a summary of information Meta has received about
17 their activity from third parties, including through the Pixel, and to disconnect that data from their
18 account. Specifically, using the Off-Facebook Activity tool, which is linked to in the Data Policy and
19 accessible via other entry points, Meta users can control or disconnect the off-Facebook activity that
20 has been associated with their Facebook account, subject to some exceptions for security and safety
21 needs. Meta users can disconnect historical third-party activity data from their account using the "Clear
22 previous history" option. They can also "turn off" storage of future connections between their
23 Facebook account and their activities off Facebook using the "Disconnect Future Activity" option.
24 Meta users can make this choice for all third-party websites or on a website-by-website basis.


25 12. In addition, Meta provides other privacy tools and resources to users of the Meta
26 services that allow them to control how data shared by third parties can be used to show them relevant
27 ads. Specifically, the "Data About Your Activity From Partners" tool within Meta's "Ad Settings"
28 allows users to opt out of receiving personalized advertisements based on their activity on third-party

1 websites, apps, or offline, among other things.

2 13. Additional tools Meta provides to its users, which enable them to control
3 advertisements they receive, include the following:

- 4 • **Hide ad:** Users can hide individual advertisements appearing in their News Feed.
- 5 • **Report ad:** Users can report advertisements in their News Feed if they consider them
6 to be inappropriate—for example, due to containing spam, false news, or being
7 misleading or sexually inappropriate.
- 8 • **Hide advertiser:** Users can hide all advertisements from a specific developer altogether
9 via their Ad Preferences.
- 10 • **Limit ad topics:** Users can limit advertisements about topics such as alcohol, parenting,
11 pets, social issues, and elections or politics, and advertisers cannot target the user based
12 on an interest in that topic.

13 I declare under penalty of perjury that the foregoing is true and correct, and that I executed this
14 Declaration on October ¹⁷, 2022, in Adelaide, South Australia.

15
16 

17 Tobias Wooldridge
18
19
20
21
22
23
24
25
26
27
28

Exhibit 1

At Meta, we have policies around the kinds of information businesses can share with us. We don't want websites or apps sending us sensitive information about people.

Business Tools Data is data sent from advertisers to Meta in connection with advertising, matching, measurement and analytics, including through the use of Business Tools, Social Plugins, Login, and certain APIs. Meta's [Business Tools Terms](#) outline the type of data that advertisers should not send to Meta via any of the Meta Business Tools.

Specifically, advertisers should not share Business Tools Data with Meta that they know or reasonably should know is either from or about children under the age of 13, or includes health or financial information, or other categories of sensitive information. This includes any information defined as sensitive under applicable laws, regulations and applicable industry guidelines.

Advertisers may use the Meta Business Tools to send to Meta information that personally identifies individuals (referred to as Contact Information), such as names, email addresses, and phone numbers, to help Meta match the data advertisers share with Meta user accounts. However, such Contact Information must be hashed in a manner specified by Meta before transmission, when using a Meta image Pixel or other Meta Business Tools. Visit [Meta for Developers](#) for hashing instructions.

Use the Learn More section below for further guidance on certain types of sensitive Business Tools Data prohibited under Meta's [Business Tools Terms](#).

If you receive a notification that you're violating Meta's Business Tools data policies, [learn how to troubleshoot the issue](#).

Learn more

GIBSON, DUNN & CRUTCHER LLP
LAUREN R. GOLDMAN (*pro hac vice*)
lgoldman@gibsondunn.com
200 Park Avenue
New York, NY 10166
Telephone: (212) 351-4000
Facsimile: (212) 351-4035

ELIZABETH K. MCCLOSKEY (SBN 268184)
emccloskey@gibsondunn.com
ABIGAIL A. BARRERA (SBN 301746)
abarrera@gibsondunn.com
555 Mission Street, Suite 3000
San Francisco, CA 94105
Telephone: (415) 393-8200
Facsimile: (415) 393-8306

TRENTON J. VAN OSS (*pro hac vice*)
tvanoss@gibsondunn.com
1050 Connecticut Avenue, N.W.
Washington, DC 20036-5306
Telephone: (202) 955-8500
Facsimile: (202) 467-0539

*Attorneys for Defendant Meta Platforms, Inc.
(formerly known as Facebook, Inc.)*

COOLEY LLP
MICHAEL G. RHODES (SBN 116127)
rhodesmg@cooley.com
KYLE C. WONG (SBN 224021)
kwong@cooley.com
CAMERON J. CLARK (SBN 313039)
cclark@cooley.com
CAROLINE A. LEBEL (SBN 340067)
clebel@cooley.com
3 Embarcadero Center, 20th Floor
San Francisco, CA 94111-4004
Telephone: (415) 693-2000
Facsimile: (415) 693-2222

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

IN RE META PIXEL HEALTHCARE
LITIGATION

This Document Relates To:

Case No. 3:22-cv-3580-WHO (Doe)

Case No. 3:22-cv-3580-WHO

PUTATIVE CLASS ACTION

**DECLARATION OF ABIGAIL A. BARRERA
IN SUPPORT OF DEFENDANT META
PLATFORMS, INC.'S OPPOSITION TO
PLAINTIFFS' MOTION FOR
PRELIMINARY INJUNCTION**

*[Opposition and Declaration of Tobias
Wooldridge filed concurrently herewith]*

Action Filed: June 17, 2022

Honorable Judge William H. Orrick

1 I, Abigail A. Barrera, declare as follows:

2 1. I am an attorney admitted to practice law in the State of California. I am an associate
3 at the law firm of Gibson, Dunn & Crutcher LLP, and I represent Meta Platforms, Inc. (“Meta”) in
4 the above-referenced action. I submit this declaration in support of Meta’s Opposition to Plaintiffs’
5 Motion for Preliminary Injunction. Unless otherwise stated, the following facts are within my
6 personal knowledge and, if called and sworn as a witness, I could and would testify competently to
7 them.

8 2. Attached hereto as **Exhibit A** is a true and correct copy of Meta’s Terms of Service
9 dated July 26, 2022.

10 3. Attached hereto as **Exhibit B** is a true and correct copy of Meta’s Data Policy dated
11 January 4, 2022.

12 4. Attached hereto as **Exhibit C** is a true and correct copy of Meta’s Cookies Policy
13 dated January 4, 2022.

14 5. Attached hereto as **Exhibit D** is a true and correct copy of Meta’s Business Tools
15 Terms dated August 31, 2020.

16 6. Attached hereto as **Exhibit E** is a true and correct copy of Meta’s Commercial Terms
17 dated January 4, 2022.

18 7. Using the Off-Facebook Activity tool, Meta users can disconnect historical third-party
19 activity data from their account using the “Clear previous history” option. They can also “turn off”
20 storage of future connections between their Facebook account and their activities off Facebook using
21 the “Disconnect Future Activity” option. Meta users can make this choice for all third-party websites
22 or on a website-by-website basis. Attached hereto as **Exhibit F** is a true and correct copy of a
23 screenshot taken on October 16, 2022 showing the available settings in a user’s “Off-Facebook
24 activity” section of the Facebook website.

25 8. Attached hereto as **Exhibit G** is a true and correct copy of an article entitled “How do
26 I disconnect my off-Facebook activity?” downloaded from Facebook’s Help Center on October 16,
27 2022.

1 9. Attached hereto as **Exhibit H** is a true and correct copy of an article entitled “How do
2 I manage my future off-Facebook activity?” downloaded from Facebook’s Help Center on October
3 16, 2022.

4 10. The “Data About Your Activity From Partners” tool within Meta’s “Ad Settings”
5 allows users to opt out of receiving personalized advertisements based on their activity on third-party
6 websites, apps, or offline, among other things. Attached hereto as **Exhibit I** is a true and correct
7 copy of a screenshot taken on October 17, 2022 showing the “Data About Your Activity From
8 Partners” tool in a user’s “Ad Preferences” section of the Facebook website.

9 11. Attached hereto as **Exhibit J** is a true and correct copy of Meta’s Privacy Policy
10 (formerly called the Data Policy) dated July 26, 2022.

11 12. Attached hereto as **Exhibit K** is a true and correct copy of Meta’s Cookies Policy
12 dated October 5, 2022.

13
14 Executed this 17th day of October, 2022 in San Francisco, California.

15
16 /s/ Abigail A. Barrera

17 Abigail A. Barrera
18
19
20
21
22
23
24
25
26
27
28

Exhibit A

[Sign Up](#)

Email or phone

Password

[Log In](#)[Forgot account?](#)

1. The services we provide

2. How our services are funded

3. Your commitments to Facebook and our community

4. Additional provisions

5. Other terms and policies that may apply to you

[Facebook Ads Controls](#)[Privacy Basics](#)[Cookies Policy](#)[Data Policy](#)[More Resources](#)

- [View a printable version of the Terms of Service](#)

The Facebook company is now Meta. We've updated our Terms of Use, Data Policy, and Cookies Policy to reflect the new name on January 4, 2022. While our company name has changed, we are continuing to offer the same products, including the Facebook app from Meta. Our Data Policy and Terms of Service remain in effect, and this name change does not affect how we use or share data. [Learn more about Meta](#) and our vision for the metaverse.

Terms of Service

Meta builds technologies and services that enable people to connect with each other, build communities, and grow businesses. These Terms govern your use of Facebook, Messenger, and the other products, features, apps, services, technologies, and software we offer (the [Meta Products or Products](#)), except where we expressly state that separate terms (and not these) apply. These Products are provided to you by Meta Platforms, Inc.

We don't charge you to use Facebook or the other products and services covered by these Terms, unless we state otherwise. Instead, businesses and organizations, and other persons pay us to show you ads for their products and services. By using our Products, you agree that we can show you ads that we think may be relevant to you and your interests. We use your personal data to help determine which personalized ads to show you.

We don't sell your personal data to advertisers, and we don't share information that directly identifies you (such as your name, email address or other contact information) with advertisers unless you give us specific permission. Instead, advertisers can tell us things like the kind of audience they want to see their ads, and we show those ads to people who may be interested. We provide advertisers with reports about the performance of their ads that help them understand how people are interacting with their content. See Section 2 below to learn more about how personalized advertising under these terms works on the Meta Products.

Our [Privacy Policy](#) explains how we collect and use your personal data to determine some of the ads you see and provide all of the other services described below. You can also go to your [settings](#) pages of the relevant Meta Product at any time to review the privacy choices you have about how we use your data.

[Return to top](#)

1. The services we provide

Our mission is to give people the power to build community and bring the world closer together. To help advance this mission, we provide the Products and services described below to you:

Provide a personalized experience for you:

Your experience on Facebook is unlike anyone else's: from the posts, stories, events, ads, and other content you see in Facebook News Feed or our video platform to the Facebook Pages you follow and other features you might use, such as Facebook Marketplace, and search. For example, we use data about the connections you make, the choices and settings you select, and what you share and do on and off our Products - to personalize your experience.

Connect you with people and organizations you care about:

We help you find and connect with people, groups, businesses, organizations, and others that matter to you across the Meta Products you use. We use data to make suggestions for you and others - for example, groups to join, events to attend, Facebook Pages to follow or send a message to, shows to watch, and people you may want to become friends with. Stronger ties make for better communities, and we believe our services are most useful when people are connected to people, groups, and organizations they care about.

Empower you to express yourself and communicate about what matters to you:

There are many ways to express yourself on Facebook to communicate with friends, family, and others about what matters to you - for example, sharing status updates, photos, videos, and stories across the Meta Products (consistent with your settings), sending messages or making voice or video calls to a friend or several people, creating events or groups, or adding content to your profile as well as showing you insights on how others engage with your content. We have also developed, and continue to explore, new ways for people to use technology, such as augmented reality and 360 video to create and share more expressive and engaging content on Meta Products.

Help you discover content, products, and services that may interest you:

We show you personalized ads, offers, and other sponsored or commercial content to help you discover content, products, and services that are offered by the many businesses and organizations that use Facebook and other Meta Products. Section 2 below explains this in more detail.

Promote the safety, security, and integrity of our services, combat harmful conduct and keep our community of users safe:

People will only build community on Meta Products if they feel safe and secure. We work hard to maintain the security (including the availability, authenticity, integrity, and confidentiality) of our Products and services. We employ dedicated teams around the world, work with external service providers, partners and other relevant entities and develop advanced technical systems to detect potential misuse of our Products, harmful conduct towards others, and situations where we may be able to help support or protect our community, including to respond to user reports of potentially violating content. If we learn of content or conduct like this, we may take appropriate action based on our assessment that may include - notifying you, offering help, removing content, removing or restricting access to certain features, disabling an account, or contacting law enforcement. We share data across Meta Companies when we detect misuse or harmful conduct by someone using one of our Products or to help keep Meta Products, users and the community safe. For example, we share information with Meta Companies that provide financial products and services to help them promote safety, security and integrity and comply with applicable law. Meta may access, preserve, use and share any information it collects about you where it has a good faith belief it is required or permitted by law to do so. For more information, please review our Privacy Policy.

In some cases, the Oversight Board may review our decisions, subject to its terms and bylaws. Learn more here.

Use and develop advanced technologies to provide safe and functional services for everyone:

We use and develop advanced technologies - such as artificial intelligence, machine learning systems, and augmented reality - so that people can use our Products safely regardless of physical ability or geographic location. For example, technology like this helps people who have visual impairments understand what or who is in photos or videos shared on Facebook or Instagram. We also build sophisticated network and communication technology to help more people connect to the internet in areas with limited access. And we develop automated systems to improve our ability to detect and remove abusive and dangerous activity that may harm our community and the integrity of our Products.

Research ways to make our services better:

We engage in research to develop, test, and improve our Products. This includes analyzing data we have about our users and understanding how people use our Products, for example by conducting surveys and testing and troubleshooting new features. Our Privacy Policy explains how we use data to support this research for the purposes of developing and improving our services.

Provide consistent and seamless experiences across the Meta Company Products:

Our Products help you find and connect with people, groups, businesses, organizations, and others that are important to you. We design our systems so that your experience is consistent and seamless across the different Meta Company Products that you use. For example, we use data about the people you engage with on Facebook to make it easier for you to connect with them on Instagram or Messenger, and we enable you to communicate with a business you follow on Facebook through

Messenger.

Ensuring access to our services:

To operate our global services and enable you to connect with people around the world, we need to transfer, store and distribute content and data to our data centers, partners, service providers, vendors and systems around the world, including outside your country of residence. The use of this global infrastructure is necessary and essential to provide our services. This infrastructure may be owned, operated, or controlled by Meta Platforms, Inc., Meta Platforms Ireland Limited, or its affiliates.

[Return to top](#)

2. How our services are funded

Instead of paying to use Facebook and the other products and services we offer, by using the Facebook Products covered by these Terms, you agree that we can show you ads that businesses and organizations pay us to promote on and off the [Facebook Company Products](#). We use your personal data, such as information about your activity and interests, to show you ads that are more relevant to you.

Protecting people's privacy is central to how we've designed our ad system. This means that we can show you relevant and useful ads without telling advertisers who you are. We don't sell your personal data. We allow advertisers to tell us things like their business goal, and the kind of audience they want to see their ads (for example, people between the age of 18-35 who like cycling). We then show their ad to people who might be interested.

We also provide advertisers with reports about the performance of their ads to help them understand how people are interacting with their content on and off Facebook. For example, we provide general demographic and interest information to advertisers (for example, that an ad was seen by a woman between the ages of 25 and 34 who lives in Madrid and likes software engineering) to help them better understand their audience. We don't share information that directly identifies you (information such as your name or email address that by itself can be used to contact you or identifies who you are) unless you give us specific permission. Learn more about how Facebook ads work [here](#).

We collect and use your personal data in order to provide the services described above to you. You can learn about how we collect and use your data in our [Data Policy](#). You have controls over the types of ads and advertisers you see, and the types of information we use to determine which ads we show you. [Learn more](#).

[Return to top](#)

3. Your commitments to Facebook and our community

and our community

We provide these services to you and others to help advance our mission. In exchange, we need you to make the following commitments:

1. Who can use Facebook

When people stand behind their opinions and actions, our community is safer and more accountable. For this reason, you must:

- Provide for your account the same name that you use in everyday life.
- Provide accurate information about yourself.
- Create only one account (your own) and use it for personal purposes.
- Not share your password, give access to your Facebook account to others, or transfer your account to anyone else (without our permission).

We try to make Facebook broadly available to everyone, but you cannot use Facebook if:

- You are under 13 years old.
- You are a convicted sex offender.
- We've previously disabled your account for violations of our Terms or the Community Standards, or other terms and policies that apply to your use of Facebook. If we disable your account for a violation of our Terms, the Community Standards, or other terms and policies, you agree not to create another account without our permission. Receiving permission to create a new account is provided at our sole discretion, and does not mean or imply that the disciplinary action was wrong or without cause.
- You are prohibited from receiving our products, services, or software under applicable laws.

2. What you can share and do on Meta Products

We want people to use Meta Products to express themselves and to share content that is important to them, but not at the expense of the safety and well-being of others or the integrity of our community. You therefore agree not to engage in the conduct described below (or to facilitate or support others in doing so):

1. You may not use our Products to do or share anything:

- That violates these Terms, the Community Standards, or other terms and policies that apply to your use of our Products.
- That is unlawful, misleading, discriminatory or fraudulent (or assists someone else in using our Products in such a way).
- That you do not own or have the necessary rights to share.
- That infringes or violates someone else's rights, including their intellectual property rights (such as by infringing another's copyright or trademark, or distributing or selling counterfeit or pirated goods), unless an exception or limitation applies under applicable law.

2. You may not upload viruses or malicious code, use the services to send spam, or do anything else that could disable, overburden, interfere with, or impair the proper working, integrity, operation, or appearance of our services, systems, or Products.
3. You may not access or collect data from our Products using automated means (without our prior permission) or attempt to access data you do not have permission to access.
4. You may not proxy, request, or collect Product usernames or passwords, or misappropriate access tokens.
5. You may not sell, license, or purchase any data obtained from us or our services, except as provided in the Platform Terms.
6. You may not misuse any reporting, flagging, dispute, or appeals channel, such as by making fraudulent, duplicative, or groundless reports or appeals.

We can remove or restrict access to content that is in violation of these provisions. We can also suspend or disable your account for conduct that violates these provisions, as provided in Section 4.B.

If we remove content that you have shared in violation of the Community Standards, we'll let you know and explain any options you have to request another review, unless you seriously or repeatedly violate these Terms or if doing so may expose us or others to legal liability; harm our community of users; compromise or interfere with the integrity or operation of any of our services, systems or Products; where we are restricted due to technical limitations; or where we are prohibited from doing so for legal reasons. For information on account suspension or termination, see Section 4.B below.

To help support our community, we encourage you to report content or conduct that you believe violates your rights (including intellectual property rights) or our terms and policies, if this feature exists in your jurisdiction.

We also can remove or restrict access to content features, services, or information if we determine that doing so is reasonably necessary to avoid or mitigate misuse of our services or adverse legal or regulatory impacts to Meta.

3. The permissions you give us

We need certain permissions from you to provide our services:

1. Permission to use content you create and share: Some content that you share or upload, such as photos or videos, may be protected by intellectual property laws.

You retain ownership of the intellectual property rights (things like copyright or trademarks) in any such content that you create and share on Facebook and other Meta Company Products you use. Nothing in these Terms takes away the rights you have to your own content. You are free to share your content with anyone else, wherever you want.

However, to provide our services we need you to give us some legal permissions (known as a "license") to use this content. This is solely for the purposes of providing and improving our Products and

services as described in Section 1 above.

Specifically, when you share, post, or upload content that is covered by intellectual property rights on or in connection with our Products, you grant us a non-exclusive, transferable, sub-licensable, royalty-free, and worldwide license to host, use, distribute, modify, run, copy, publicly perform or display, translate, and create derivative works of your content (consistent with your privacy and application settings). This means, for example, that if you share a photo on Facebook, you give us permission to store, copy, and share it with others (again, consistent with your settings) such as Meta Products or service providers that support those products and services. This license will end when your content is deleted from our systems.

You can delete individual content you share, post, and upload at any time. In addition, all content posted to your personal account will be deleted if you delete your account. Learn more about how to delete your account. Account deletion does not automatically delete content that you post as an admin of a page or content that you create collectively with other users, such as photos in Shared Albums which may continue to be visible to other album members.

It may take up to 90 days to delete content after we begin the account deletion process or receive a content deletion request. If you send content to trash, the deletion process will automatically begin in 30 days unless you chose to delete the content sooner. While the deletion process for such content is being undertaken, the content is no longer visible to other users. After the content is deleted, it may take us up to another 90 days to remove it from backups and disaster recovery systems.

Content will not be deleted within 90 days of the account deletion or content deletion process beginning in the following situations:

- where your content has been used by others in accordance with this license and they have not deleted it (in which case this license will continue to apply until that content is deleted);
- where deletion within 90 days is not possible due to technical limitations of our systems, in which case, we will complete the deletion as soon as technically feasible; or
- where immediate deletion would restrict our ability to:
 - investigate or identify illegal activity or violations of our terms and policies (for example, to identify or investigate misuse of our Products or systems);
 - protect the safety, integrity, and security of our Products, systems, services, our employees, and users, and to defend ourselves;
 - comply with legal obligations for the preservation of evidence, including data Meta Companies providing financial products and services preserve to comply with any record keeping obligations required by law; or
 - comply with a request of a judicial or administrative authority, law enforcement or a government agency;

in which case, the content will be retained for no longer than is necessary for the purposes for which it has been retained (the exact duration will vary on a case-by-case basis).

In each of the above cases, this license will continue until the content has been fully deleted.

2. Permission to use your name, profile picture, and information about your actions with ads and sponsored or commercial content:

You give us permission to use your name and profile picture and information about actions you have taken on Facebook next to or in connection with ads, offers, and other sponsored or commercial content that we display across our Products, without any compensation to you. For example, we may show your friends that you are interested in an advertised event or have liked a Facebook Page created by a brand that has paid us to display its ads on Facebook. Ads and content like this can be seen only by people who have your permission to see the actions you've taken on Meta Products. You can [learn more](#) about your ad settings and preferences.

3. Permission to update software you use or download: If you download or use our software, you give us permission to download and install updates to the software where available.

4. Limits on using our intellectual property

If you use content covered by intellectual property rights that we have and make available in our Products (for example, images, designs, videos, or sounds we provide that you add to content you create or share on Facebook), we retain all rights to that content (but not yours). You can only use our copyrights or trademarks (or any similar marks) as expressly permitted by our [Brand Usage Guidelines](#) or with our prior written permission. You must obtain our written permission (or permission under an open source license) to modify, translate, create derivative works of, decompile, or reverse engineer our products or their components, or otherwise attempt to extract source code from us, unless an exception or limitation applies under applicable law or your conduct relates to the [Meta Bug Bounty Program](#).

[Return to top](#)

4. Additional provisions

1. Updating our Terms

We work constantly to improve our services and develop new features to make our Products better for you and our community. As a result, we may need to update these Terms from time to time to accurately reflect our services and practices, to promote a safe and secure experience on our Products and services, and/or to comply with applicable law. Unless otherwise required by law, we will notify you before we make changes to

changes requested by us, we will notify you before the changes to these Terms and give you an opportunity to review them before they go into effect. Once any updated Terms are in effect, you will be bound by them if you continue to use our Products.

We hope that you will continue using our Products, but if you do not agree to our updated Terms and no longer want to be a part of the Facebook community, you can delete your account at any time.

2. Account suspension or termination

We want Facebook to be a place where people feel welcome and safe to express themselves and share their thoughts and ideas.

If we determine, in our discretion, that you have clearly, seriously or repeatedly breached our Terms or Policies, including in particular the Community Standards, we may suspend or permanently disable your access to Meta Company Products, and we may permanently disable or delete your account. We may also disable or delete your account if you repeatedly infringe other people's intellectual property rights or where we are required to do so for legal reasons.

We may disable or delete your account if after registration your account is not confirmed, your account is unused and remains inactive for an extended period of time, or if we detect someone may have used it without your permission and we are unable to confirm your ownership of the account. Learn more about how we disable and delete accounts.

Where we take such action we'll let you know and explain any options you have to request a review, unless doing so may expose us or others to legal liability; harm our community of users; compromise or interfere with the integrity or operation of any of our services, systems or Products; where we are restricted due to technical limitations; or where we are prohibited from doing so for legal reasons.

You can learn more about what you can do if your account has been disabled and how to contact us if you think we have disabled your account by mistake.

If you delete or we disable or delete your account, these Terms shall terminate as an agreement between you and us, but the following provisions will remain in place: 3, 4.2-4.5.

3. Limits on liability

We work hard to provide the best Products we can and to specify clear guidelines for everyone who uses them. Our Products, however, are provided "as is," and we make no guarantees that they always will be safe, secure, or error-free, or that they will function without disruptions, delays, or imperfections. To the extent permitted by law, we also DISCLAIM ALL WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT. We do not control or direct what people and others do or say, and we are not responsible for their actions or conduct (whether online or offline) or any content they share (including offensive, inappropriate, obscene, unlawful, and other objectionable content).

We cannot predict when issues might arise with our Products. Accordingly, our liability shall be limited to the fullest extent permitted by applicable law, and under no circumstance will we be liable to you for any lost profits, revenues, information, or data, or consequential, special,

...promises, services, information or data, or consequently, special, indirect, exemplary, punitive, or incidental damages arising out of or related to these Terms or the Meta Products (however caused and on any theory of liability, including negligence), even if we have been advised of the possibility of such damages. Our aggregate liability arising out of or relating to these Terms or the Meta Products will not exceed the greater of \$100 or the amount you have paid us in the past twelve months.

4. Disputes

We try to provide clear rules so that we can limit or hopefully avoid disputes between you and us. If a dispute does arise, however, it's useful to know up front where it can be resolved and what laws will apply.

You and Meta each agree that any claim, cause of action, or dispute between us that arises out of or relates to these Terms or your access or use of the Meta Products shall be resolved exclusively in the U.S. District Court for the Northern District of California or a state court located in San Mateo County. You also agree to submit to the personal jurisdiction of either of these courts for the purpose of litigating any such claim, and that the laws of the State of California will govern these Terms and any claim, cause of action, or dispute without regard to conflict of law provisions. Without prejudice to the foregoing, you agree that, in its sole discretion, Meta may bring any claim, cause of action, or dispute we have against you in any competent court in the country in which you reside that has jurisdiction over the claim.

5. Other

1. These Terms (formerly known as the Statement of Rights and Responsibilities) make up the entire agreement between you and Meta Platforms, Inc. regarding your use of our Products. They supersede any prior agreements.
2. Some of the Products we offer are also governed by supplemental terms. If you use any of those Products, supplemental terms will be made available and will become part of our agreement with you. For instance, if you access or use our Products for commercial or business purposes, such as buying ads, selling products, developing apps, managing a group or Page for your business, or using our measurement services, you must agree to our [Commercial Terms](#). If you post or share content containing music, you must comply with our [Music Guidelines](#). To the extent any supplemental terms conflict with these Terms, the supplemental terms shall govern to the extent of the conflict.
3. If any portion of these Terms is found to be unenforceable, the unenforceable portion will be deemed amended to the minimum extent necessary to make it enforceable, and if it can't be made enforceable, then it will be severed and the remaining portion will remain in full force and effect. If we fail to enforce any of these Terms, it will not be considered a waiver. Any amendment to or waiver of these Terms must be made in writing and signed by us.
4. You will not transfer any of your rights or obligations under these Terms to anyone else without our consent.
5. You may designate a person (called a legacy contact) to manage your account if it is memorialized. If you enable it in your settings, only your legacy contact or a person who you have identified in a

valid will or similar legal document expressing clear consent to disclose your content to that person upon death or incapacity will be able to seek limited disclosure of information from your account after it is memorialized.

6. These Terms do not confer any third-party beneficiary rights. All of our rights and obligations under these Terms are freely assignable by us in connection with a merger, acquisition, or sale of assets, or by operation of law or otherwise.
7. We may need to change the username for your account in certain circumstances (for example, if someone else claims the username and it appears unrelated to the name you use in everyday life).
8. We always appreciate your feedback and other suggestions about our products and services. But we may use feedback and other suggestions without any restriction or obligation to compensate you, and we are under no obligation to keep them confidential.
9. We reserve all rights not expressly granted to you.

[Return to top](#)

5. Other terms and policies that may apply to you

- Community Standards: These guidelines outline our standards regarding the content you post to Facebook and your activity on Facebook and other Meta Products.
- Commercial Terms: These terms apply if you also access or use our Products for any commercial or business purpose, including advertising, operating an app on our Platform, using our measurement services, managing a group or a Page for a business, or selling goods or services.
- Community Payment Terms: These terms apply to payments made on or through Meta Products.
- Commerce Policies: These guidelines outline the policies that apply when you offer products or services for sale on Facebook, Instagram, and WhatsApp.
- Music Guidelines: These guidelines outline the policies that apply if you post or share content containing music on any Meta Products.
- Advertising Policies: These policies apply to partners who advertise across the Meta Products and specify what types of ad content are allowed by partners who advertise across the Meta Products.
- Self-Serve Ad Terms: These terms apply when you use self-serve advertising interfaces to create, submit, or deliver advertising or other commercial or sponsored activity or content.
- Facebook Pages, Groups and Events Policy: These guidelines apply if you create or administer a Facebook Page, group, or event, or if you use Facebook to communicate or administer a promotion.

- [Meta Platform Policy](#): These terms apply to the use of the set of APIs, SDKs, tools, plugins, code, technology, content, and services that enables others to develop functionality, retrieve data from MetaProducts, or provide data to us.
- [Developer Payment Terms](#): These terms apply to developers of applications that use Facebook Payments.
- [Meta Brand Resources](#): These guidelines outline the policies that apply to use of Meta trademarks, logos, and screenshots.
- [Recommendations Guidelines](#): The [Facebook Recommendations Guidelines](#) and [Instagram Recommendations Guidelines](#) outline our standards for recommending and not recommending content.
- [Live Policies](#): These policies apply to all content broadcast to Facebook Live.

Date of Last Revision: July 26, 2022

[English \(US\)](#) [Español](#) [Français \(France\)](#) [中文\(简体\)](#) [العربية](#) [Português \(Brasil\)](#) [Italiano](#) [한국어](#) [Deutsch](#) [हिन्दी](#) [日本語](#)

[Sign Up](#) [Log In](#) [Messenger](#) [Facebook Lite](#) [Watch](#) [Places](#) [Games](#) [Marketplace](#) [Facebook Pay](#) [Oculus](#) [Portal](#) [Instagram](#) [Bulletin](#) [Local](#)
[Fundraisers](#) [Services](#) [Voting Information Center](#) [Groups](#) [About](#) [Create Ad](#) [Create Page](#) [Developers](#) [Careers](#) [Privacy](#) [Cookies](#) [Ad choices](#) [Terms](#)
[Help](#) [Contact](#) [Uploading & Non-Users](#)

Meta © 2022

Exhibit B

We've updated our policy. [Read it here.](#)

The Facebook company is now Meta. We've updated our Terms of Use, Data Policy, and Cookies Policy to reflect the new name on January 4, 2022. While our company name has changed, we are continuing to offer the same products, including the Facebook app from Meta. Our Data Policy and Terms of Service remain in effect, and this name change does not affect how we use or share data. Learn more about Meta and our vision for the metaverse.

Data Policy

This policy describes the information we process to support Facebook, Instagram, Messenger and other products and features offered by Meta Platforms, Inc. (Meta Products or Products). You can find additional tools and information in the Facebook Settings and Instagram Settings.

What kinds of information do we collect?

How do we use this information?

How is this information shared?

How do the Meta Companies work together?

How can I manage or delete information about me?

How do we respond to legal requests or prevent harm?

How do we operate and transfer data as part of our global services?

How will we notify you of changes to this policy?

Privacy notice for California residents

How to contact us with questions

Facebook Ads Controls

Privacy Basics

Cookies Policy

Terms

More Resources

View a printable version of the Data Policy

Interactive Tools

Minors and Safety

Facebook Privacy Page

Facebook Safety Page

Facebook Site Governance Page

EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Notice

[Return to top](#)

What kinds of information do we collect?

To provide the Meta Products, we must process information about you. The types of information we collect depend on how you use our Products. You can learn how to access and delete information we collect by visiting the Facebook Settings and Instagram Settings.

Things you and others do and provide.

- **Information and content you provide.** We collect the content, communications and other information you provide when you use our Products, including when you sign up for an account, create or share content, and message or communicate with others. This can include information in or about the content you provide (like metadata), such as the location of a photo or the date a file was created. It can also include what you see through features we provide, such as our camera, so we can do things like suggest masks and filters that you might like, or give you tips on using camera formats. Our systems automatically process content and communications you and others provide to analyze context and what's in them for the purposes described below. Learn more about how you can control who can see the things you share.
 - **Data with special protections:** You can choose to provide information in your Facebook profile fields or Life Events about your religious views, political views, who you are "interested in," or your health. This and other information (such as racial or ethnic origin, philosophical beliefs or trade union membership) could be subject to special protections under the laws of your country.
- **Networks and connections.** We collect information about the people, accounts, hashtags and Facebook groups, and Pages you are connected to and how you interact with them across our Products, such as people you communicate with the most or groups you are part of. We also collect contact information if you choose to upload, sync or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping you and others find people you may know and for the other purposes listed below.
- **Your usage.** We collect information about how you use our Products, such as the types of content you view or engage with; the features you use; the actions you take; the people or accounts you interact with; and the time, frequency and duration of your activities. For example, we log when you're using and have last used our Products, and what posts, videos and other content you view on our Products. We also collect information about how you use features like our camera.
- **Information about transactions made on our Products.** If you use our Products for purchases or other financial transactions (such as when you make a purchase in a game or make a donation), we collect information about the purchase or transaction. This includes payment information, such as your credit or debit card number and other card information; other account and authentication information; and billing, shipping and contact details.
- **Things others do and information they provide about you.** We also receive and analyze content, communications and information that other people provide when they use our Products. This can

include information about you, such as when others share or comment on a photo of you, send a message to you, or upload, sync or import your contact information.

Device Information

As described below, we collect information from and about the computers, phones, connected TVs and other web-connected devices you use that integrate with our Products, and we combine this information across different devices you use. For example, we use information collected about your use of our Products on your phone to better personalize the content (including ads) or features you see when you use our Products on another device, such as your laptop or tablet, or to measure whether you took an action in response to an ad we showed you on your phone on a different device.

Information we obtain from these devices includes:

- **Device attributes:** information such as the operating system, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins.
- **Device operations:** information about operations and behaviors performed on the device, such as whether a window is foregrounded or backgrounded, or mouse movements (which can help distinguish humans from bots).
- **Identifiers:** unique identifiers, device IDs, and other identifiers, such as from games, apps or accounts you use, and Family Device IDs (or other identifiers unique to Meta Company Products associated with the same device or account).
- **Device signals:** Bluetooth signals, and information about nearby Wi-Fi access points, beacons, and cell towers.
- **Data from device settings:** information you allow us to receive through device settings you turn on, such as access to your GPS location, camera or photos.
- **Network and connections:** information such as the name of your mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, in some cases, information about other devices that are nearby or on your network, so we can do things like help you stream a video from your phone to your TV.
- **Cookie data:** data from cookies stored on your device, including cookie IDs and settings. Learn more about how we use cookies in the Facebook Cookies Policy and Instagram Cookies Policy.

Information from partners.

Advertisers, app developers, and publishers can send us information through Meta Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Meta pixel. These partners provide information about your activities off of our Products—including information about your device, websites you visit, purchases you make, the ads you see, and how you use their services—

whether or not you have an account or are logged into our Products. For example, a game developer could use our API to tell us what games you play, or a business could tell us about a purchase you made in its store. We also receive information about your online and offline actions and purchases from third-party data providers who have the rights to provide us with your information.

Partners receive your data when you visit or use their services or through third parties they work with. We require each of these partners to have lawful rights to collect, use and share your data before providing any data to us. Learn more about the types of partners we receive data from.

To learn more about how we use cookies in connection with Meta Business Tools, review the Facebook Cookies Policy and Instagram Cookies Policy.

[Return to top](#)

How do we use this information?

We use the information we have (subject to choices you make) as described below and to provide and support the Meta Products and related services described in the Meta Terms and Instagram Terms. Here's how:

Provide, personalize and improve our Products.

We use the information we have to deliver our Products, including to personalize features and content (including your ads, Facebook News Feed, Instagram Feed, and Instagram Stories) and make suggestions for you (such as groups or events you may be interested in or topics you may want to follow) on and off our Products. To create personalized Products that are unique and relevant to you, we use your connections, preferences, interests and activities based on the data we collect and learn from you and others (including any data with special protections you choose to provide); how you use and interact with our Products; and the people, places, or things you're connected to and interested in on and off our Products. Learn more about how we use information about you to personalize your Facebook and Instagram experience, including features, content and recommendations in Meta Products; you can also learn more about how we choose the ads that you see.

- **Information across Meta Products and devices:** We connect information about your activities on different Meta Products and devices to provide a more tailored and consistent experience on all Meta Products you use, wherever you use them. For example, we can suggest that you join a group on Facebook that includes people you follow on Instagram or communicate with using Messenger.

We can also make your experience more seamless, for example, by automatically filling in your registration information (such as your phone number) from one Meta Product when you sign up for an account on a different Product.

- **Location-related information:** We use location-related information-such as your current location, where you live, the places you like to go, and the businesses and people you're near-to provide, personalize and improve our Products, including ads, for you and others. Location-related information can be based on things like precise device location (if you've allowed us to collect it), IP addresses, and information from your and others' use of Meta Products (such as check-ins or events you attend).
- **Product research and development:** We use the information we have to develop, test and improve our Products, including by conducting surveys and research, and testing and troubleshooting new products and features.
- **Ads and other sponsored content:** We use the information we have about you-including information about your interests, actions and connections-to select and personalize ads, offers and other sponsored content that we show you. Learn more about how we select and personalize ads, and your choices over the data we use to select ads and other sponsored content for you in the Facebook Settings and Instagram Settings.

Provide measurement, analytics, and other business services.

We use the information we have (including your activity off our Products, such as the websites you visit and ads you see) to help advertisers and other partners measure the effectiveness and distribution of their ads and services, and understand the types of people who use their services and how people interact with their websites, apps, and services. Learn how we share information with these partners.

Promote safety, integrity and security.

We use the information we have to verify accounts and activity, combat harmful conduct, detect and prevent spam and other bad experiences, maintain the integrity of our Products, and promote safety and security on and off of Meta Products. For example, we use data we have to investigate suspicious activity or violations of our terms or policies, or to detect when someone needs help. To learn more, visit the Facebook Security Help Center and Instagram Security Tips.

Communicate with you.

We use the information we have to send you marketing communications, communicate with you about our Products, and let you know about our policies and terms. We also use your information to respond to you when you contact us.

Research and innovate for social good.

We use the information we have (including from research partners we collaborate with) to conduct and support research and innovation on topics of general social welfare, technological advancement, public interest, health and well-being. For example, we analyze information we have about migration patterns during crises to aid relief efforts. Learn more about our research programs.

[Return to top](#)

How is this information shared?

Your information is shared with others in the following ways:

Sharing on Meta Products

People and accounts you share and communicate with

When you share and communicate using our Products, you choose the audience for what you share. For example, when you post on Facebook, you select the audience for the post, such as a group, all of your friends, the public, or a customized list of people. Similarly, when you use Messenger or Instagram to communicate with people or businesses, those people and businesses can see the content you send. Your network can also see actions you have taken on our Products, including engagement with ads and sponsored content. We also let other accounts see who has viewed their Facebook or Instagram Stories.

Public information can be seen by anyone, on or off our Products, including if they don't have an account. This includes your Instagram username; any information you share with a public audience; information in your public profile on Facebook; and content you share on a Facebook Page, public Instagram account or any other public forum, such as Facebook Marketplace. You, other people using Facebook and Instagram, and we can provide access to or send public information to anyone on or off our Products, including in other Meta Company Products, in search results, or through tools and APIs. Public information can also be seen, accessed, reshared or downloaded through third-party services such as search engines, APIs, and offline media such as TV, and by apps, websites and other services that integrate with our Products.

Learn more about what information is public and how to control your visibility on Facebook and Instagram.

Content others share or reshare about you

You should consider who you choose to share with, because people who can see your activity on our Products can choose to share it with others on and off our Products, including people and businesses outside the audience you shared with. For example, when you share a post or send a message to specific friends or accounts, they can download, screenshot, or reshare that content to others across or off our Products, in person or in virtual reality experiences such as Horizon Worlds. Also, when you comment on someone else's post or react to their content, your comment or reaction is visible to anyone who can see the other person's content, and that person can change the audience later.

People can also use our Products to create and share content about you with the audience they choose. For example, people can share a photo of you in a Story, mention or tag you at a location in a post, or share information about you in their posts or messages. If you are uncomfortable with what others have shared about you on our Products, you can learn how to report the content.

Information about your active status or presence on our Products.

People in your networks can see signals telling them whether you are active on our Products, including whether you are currently active on Instagram, Messenger or Facebook, or when you last used our Products.

Apps, websites, and third-party integrations on or using our Products.

When you choose to use third-party apps, websites, or other services that use, or are integrated with, our Products, they can receive information about what you post or share. For example, when you play a game with your Facebook friends or use a Facebook Comment or Share button on a website, the game developer or website can receive information about your activities in the game or receive a comment or link that you share from the website on Facebook. Also, when you download or use such third-party services, they can access your public profile on Facebook, and any information that you share with them. Apps and websites you use may receive your list of Facebook friends if you choose to share it with them. But apps and websites you use will not be able to receive any other information about your Facebook friends from you, or information about any of your Instagram followers (although your friends and followers may, of course, choose to share this information themselves). Information collected by these third-party services is subject to their own terms and policies, not this one.

Devices and operating systems providing native versions of Facebook and Instagram (i.e. where we have not developed our own first-party apps) will have access to all information you choose to share with them, including information your friends share with you, so they can provide our core functionality to you.

Note: We are in the process of restricting developers' data access even further to help prevent abuse. For example, we will remove developers' access to your Facebook and Instagram data if you haven't used their app in 3 months, and we are changing Login, so that in the next version, we will reduce the data that an app can request without app review to include only name, Instagram username and bio, profile photo and email address. Requesting any other data will require our approval.

New owner.

If the ownership or control of all or part of our Products or their assets changes, we may transfer your information to the new owner.

Sharing with Third-Party Partners

We work with third-party partners who help us and improve our Products or who use Meta Business Tools to grow their businesses, which makes it possible to operate our companies and provide free services to people around the world. We don't sell any of your information to anyone, and we never will. We also impose strict restrictions on how our partners can use and disclose the data we provide. Here are the types of third parties we share information with:

Partners who use our analytics services.

We provide aggregated statistics and insights that help people and businesses understand how people are engaging with their posts, listings, Facebook Pages, videos and other content on and off the Meta Products. For example, Facebook Page admins and Instagram business profiles receive information about the number of people or accounts who viewed, reacted to, or commented on their posts, as well as aggregate demographic and other information that helps them understand interactions with their account or Facebook Page.

Advertisers.

We provide advertisers with reports about the kinds of people seeing their ads and how their ads are performing, but we don't share information that personally identifies you (information such as your name or email address that by itself can be used to contact you or identifies who you are) unless you give us permission. For example, we provide general demographic and interest information to advertisers (for example, that an ad was seen by a woman between the ages of 25 and 34 who lives in Madrid and likes software engineering) to help them better understand their audience. We also confirm which ads led you to make a purchase or take an action with an advertiser.

Measurement partners.

We share information about you with companies that aggregate it to provide analytics and measurement reports to our partners.

Partners offering goods and services in our Products.

When you subscribe to receive premium content, or buy something from a seller in our Products, the content creator or seller can receive your public information and other information you share with them, as well as the information needed to complete the transaction, including shipping and contact details.

Vendors and service providers.

We provide information and content to vendors and service providers who support our business, such as by providing technical infrastructure services, analyzing how our Products are used, providing customer service, facilitating payments or conducting surveys.

Researchers and academics.

We also provide information and content to research partners and academics to conduct research that advances scholarship and innovation that support our business or mission, and enhances discovery and innovation on topics of general social welfare, technological advancement, public interest, health and well-being.

Law enforcement or legal requests.

We share information with law enforcement or in response to legal requests in the circumstances outlined below.

Learn more about how you can control the information about you that you or others share with third-party partners in the Facebook Settings and Instagram Settings.

[Return to top](#)

How do the Meta Companies work together?

Facebook and Instagram share infrastructure, systems and technology with other Meta Companies (which include WhatsApp and Oculus) to provide an innovative, relevant, consistent and safe experience across all Meta Company Products you use. We also process information about you across the Meta Companies for these purposes, as permitted by applicable law and in accordance with their terms and policies. For example, we process information from WhatsApp about accounts sending spam on its service so we can take appropriate action against those accounts on Facebook, Instagram or Messenger. We also work to understand how people use and interact with Meta Company Products, such as understanding the number of unique users on different Meta Company Products.

[Return to top](#)

How can I manage or delete information about me?

We provide you with the ability to access, rectify, port and erase your data. Learn more in your Facebook Settings and Instagram Settings.

We store data until it is no longer necessary to provide our services and Meta Products, or until your account is deleted - whichever comes first. This is a case-by-case determination that depends on things like the nature of the data, why it is collected and processed, and relevant legal or operational retention needs. For example, when you search for something on Facebook, you can access and delete that query from within your search history at any time, but the log of that search is deleted after 6 months. If you submit a copy of your government-issued ID for account verification purposes, we delete that copy 30 days after review, unless otherwise stated. Learn more about deletion of content you have shared and cookie data obtained through social plugins.

When you delete your account, we delete things you have posted, such as your photos and status updates, and you won't be able to recover that information later. Information that others have shared about you isn't part of your account and won't be deleted. If you don't want to delete your account but want to temporarily stop using the Products, you can deactivate your account instead. To delete your account at any time, please visit the Facebook Settings and Instagram Settings.

[Return to top](#)

How do we respond to legal requests or prevent harm?

We access, preserve and share your information with regulators, law enforcement or others:

- In response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so. This may include responding to legal requests from jurisdictions outside of the United States when we have a good-faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards.
- When we have a good-faith belief it is necessary to: detect, prevent and address fraud, unauthorized use of the Products, violations of our terms or policies, or other harmful or illegal activity; to protect ourselves (including our rights, property or Products), you or others, including as part of investigations or regulatory inquiries; or to prevent death or imminent bodily harm. For example, if relevant, we provide information to and receive information from third-party partners about the reliability of your account to prevent fraud, abuse and other harmful activity on and off our Products.

Information we receive about you (including financial transaction data related to purchases made on our Products) can be accessed and preserved for an extended period when it is the subject of a legal request or obligation, governmental investigation, or investigations of possible violations of our terms or policies, or otherwise to prevent harm. We also retain information from accounts disabled for terms violations for at least a year to prevent repeat abuse or other term violations.

[Return to top](#)

How do we operate and transfer data as part of our global services?

We share information globally, both internally within the Meta Companies, and externally with our partners and with those you connect and share with around the world in accordance with this policy. Your information may, for example, be transferred or transmitted to, or stored and processed in the United States or other countries outside of where you live for the purposes as described in this policy. These data transfers are necessary to provide the services set forth in the Meta Terms and Instagram Terms and to globally operate and provide our Products to you. We utilize standard contract clauses, rely on the European Commission's adequacy decisions about certain countries, as applicable, and obtain your consent for these data transfers to the United States and other countries.

[Return to top](#)

How will we notify you of changes to this policy?

We'll notify you before we make changes to this policy and give you the opportunity to review the revised policy before you choose to continue using our Products.

[Return to top](#)

Privacy notice for California residents

If you are a California resident, you can learn more about your consumer privacy rights by reviewing the California Privacy Notice.

[Return to top](#)

How to contact us with questions

You can learn more about how privacy works on Facebook and on Instagram. If you have questions about this policy, you can contact us as described below.

Contact Us

You can contact us online or by mail at:

Meta Platforms, Inc.
ATTN: Privacy Operations
1601 Willow Road
Menlo Park, CA 94025

Date of Last Revision: January 4, 2022

Exhibit C

[Sign Up](#)

Email or phone

Password

[Log In](#)[Forgot account?](#)

> Why do we use cookies?



> Where do we use cookies?



> Do other Companies use cookies in connection with the Meta Products?



> How can you control your Information?

More Resources

- [Printable Cookies Policy](#)
- [Data Policy](#)
- [Terms](#)
- [Facebook Ads Settings](#)
- [Privacy Basics](#)

The Facebook company is now Meta. We've updated our [Terms of Use](#), [Data Policy](#), and [Cookies Policy](#) to reflect the new name on January 4, 2022. While our company name has changed, we are continuing to offer the same products, including the Facebook app from Meta. Our [Data Policy](#) and [Terms of Service](#) remain in effect, and this name change does not affect how we use or share data. [Learn more about Meta](#) and our vision for the metaverse.

Cookies & other storage technologies

Cookies are small pieces of text used to store information on web browsers. Cookies are used to store and receive identifiers and other information on computers, phones and other devices. Other technologies, including data that we store on your web browser or device, identifiers associated with your device and other software, are used for similar purposes. In this policy, we refer to all of these technologies as “cookies”.

We use cookies if you have a Facebook account, use the [Meta Products](#), including our website and apps, or visit other websites and apps that use the Meta Products (including the Like button). Cookies enable Meta to offer the Meta Products to you and to understand the information that we receive about you, including information about your use of other websites and apps, whether or not you are registered or logged in.

This policy explains how we use cookies and the choices you have. Except as otherwise stated in this policy, the [Data Policy](#) will apply to our processing of the data that we collect via cookies.

[Return to top](#)

Why do we use cookies?

Cookies help us provide, protect and improve the Meta Products, such as by personalising content, tailoring and measuring ads, and providing a safer experience. The cookies that we use include session cookies, which are deleted when you close your browser, and persistent cookies, which stay in your browser until they expire or you delete them. While the cookies that we use may change from time to time as we improve and update the Meta Products, we use them for

the following purposes:

Authentication

We use cookies to verify your account and determine when you're logged in so that we can make it easier for you to access the Meta Products and show you the appropriate experience and features.

For example: We use cookies to keep you logged in as you navigate between Facebook Pages. Cookies also help us remember your browser so you don't have to keep logging in to Facebook and so you can more easily log in to Facebook via third-party apps and websites. For example, we use the "c_user" and "xs" cookies, including for this purpose, which have a lifespan of 365 days.

Security, site and product integrity

We use cookies to help us keep your account, data and the Meta Products safe and secure.

For example: Cookies can help us identify and impose additional security measures when someone may be attempting to access a Facebook account without authorisation, for instance, by rapidly guessing different passwords. We also use cookies to store information that allows us to recover your account in the event that you forget your password or to require additional authentication if you tell us that your account has been hacked. This includes, for example, our "sb" and "dbln" cookies, which enable us to identify your browser securely.

We also use cookies to combat activity that violates our policies or otherwise degrades our ability to provide the Meta Products.

For example: Cookies help us fight spam and phishing attacks by enabling us to identify computers that are used to create large numbers of fake Facebook accounts. We also use cookies to detect computers infected with malware and to take steps to prevent them from causing further harm. Our "csrf" cookie, for example, helps us prevent cross-site request forgery attacks. Cookies also help us prevent underage people from registering for Facebook accounts.

Advertising, recommendations, insights and measurement

We use cookies to help us show ads and to make recommendations for businesses and other organisations to people who may be interested in the products, services or causes they promote.

For example: Cookies allow us to help deliver ads to people who have previously visited a business's website, purchased its products or used its apps and to recommend products and services based on that activity. Cookies also allow us to limit the number of times that you see an ad so you don't see the same ad over and over again. For example, the "fr" cookie is used to deliver, measure and improve the relevancy of ads, with a lifespan of 90 days.

We also use cookies to help measure the performance of ad campaigns for businesses that use the Meta Products.

For example: We use cookies to count the number of times that an ad is shown and to calculate the cost of those ads. We also use cookies to measure how often people do things, such as make a purchase following an ad impression. For example, the “_fbp” cookie identifies browsers for the purposes of providing advertising and site analytics services and has a lifespan of 90 days.

Cookies help us serve and measure ads across different browsers and devices used by the same person.

For example: We can use cookies to prevent you from seeing the same ad over and over again across the different devices that you use.

Cookies also allow us to provide insights about the people who use the Meta Products, as well as the people who interact with the ads, websites and apps of our advertisers and the businesses that use the Meta Products.

For example: We use cookies to help businesses understand the kinds of people who like their Facebook Page or use their apps so that they can provide more relevant content and develop features that are likely to be interesting to their customers.

We also use cookies, such as our “oo” cookie, which has a lifespan of five years, to help you opt out of seeing ads from Meta based on your activity on third-party websites. [Learn more](#) about the information we receive, how we decide which ads to show you on and off the Meta Products and the controls that are available to you.

Site features and services

We use cookies to enable the functionality that helps us provide the Meta Products.

For example: Cookies help us store preferences, know when you’ve seen or interacted with Meta Products’ content and provide you with customised content and experiences. For instance, cookies allow us to make suggestions to you and others, and to customise content on third-party sites that integrate our social plugins. If you are a Facebook Page administrator, cookies allow you to switch between posting from your personal Facebook account and the Facebook Page. We use cookies such as the session-based “presence” cookie to support your use of Messenger chat windows.

We also use cookies to help provide you with content relevant to your locale.

For example: We store information in a cookie that is placed on your browser or device so that you will see the site in your preferred language.

Performance

We use cookies to provide you with the best experience possible.

For example: Cookies help us route traffic between servers and understand how quickly Meta Products load for different people. Cookies also help us record the ratio and dimensions of your screen and windows and know whether you've enabled high-contrast mode, so that we can render our sites and apps correctly. For example, we set the "dpr" and "wd" cookies, each with a lifespan of 7 days, for purposes including to deliver an optimal experience for your device's screen.

Analytics and research

We use cookies to better understand how people use the Meta Products so that we can improve them.

For example: Cookies can help us understand how people use the Facebook service, analyse which parts of our Products people find most useful and engaging, and identify features that could be improved.

Third-party websites and apps

Our business partners may also choose to share information with Meta from cookies set in their own websites' domains, whether or not you have a Facebook account or are logged in. Specifically, cookies named _fbclid or _fbp may be set on the domain of the business partner whose site you're visiting. Unlike cookies that are set on Meta's own domains, these cookies aren't accessible by Meta when you're on a site other than the one on which they were set, including when you are on one of our domains. They serve the same purposes as cookies set in Meta's own domain, which are to personalise content (including ads), measure ads, produce analytics and provide a safer experience, as set out in this Cookies Policy.

[Return to top](#)

Where do we use cookies?

We may place cookies on your computer or device and receive information stored in cookies when you use or visit:

- The [Meta Products](#);
- Products provided by other members of the [Meta Companies](#); and
- Websites and apps provided by other companies that use the Meta Products, including companies that incorporate Meta technologies into their websites and apps. Meta uses cookies and receives information when you visit those sites and apps, including [device information](#) and information about your activity, without any further action from you. This occurs whether or not you have a Facebook

any further action from you. This occurs whether or not you have a Facebook account or are logged in.

[Return to top](#)

Do other Companies use cookies in connection with the Meta Products?

Yes, other companies use cookies on the Meta Products to provide advertising, measurement, marketing and analytics services to us, and to provide certain features and improve our services for you.

For example, other companies' cookies help tailor ads off of Meta Products, measure their performance and effectiveness and support marketing and analytics. Certain features on the Meta Products use cookies from other companies to function, for example, certain maps, payment and security features. [Learn more](#) about the companies that use cookies on the Meta Products.

Third party companies also use cookies on their own sites and apps in connection with the Meta Products. To understand how other companies use cookies, please review their policies.

[Return to top](#)

How can you control your Information?

We use cookies to help personalise and improve content and services, provide a safer experience and to show you useful and relevant ads on and off Meta Products. You can control how we use data to show you ads and more by using the tools described below.

If you have a Facebook account:

- You can use your [ad preferences](#) to learn why you're seeing a particular ad and control how we use information that we collect to show you ads.
- To show you better ads, we use data that advertisers and other partners provide us about your activity off Meta Company Products, including websites and apps. You can control whether we use this data to show you ads in your [ad settings](#).
- The Meta Audience Network is a way for advertisers to show you ads in apps and websites off the [Meta Company Products](#). One of the ways that Audience Network shows relevant ads is by using your ad preferences to determine which ads you may be interested in seeing.

You can control this in your [ad settings](#).

- You can review your Off-Facebook activity, which is a summary of activity that businesses and organisations share with us about your interactions with them, such as visiting their apps or websites. They use our [business tools](#), such as Meta Pixel, to share this information with us. This helps us do things like give you a more personalised experience on Meta Products. Learn more [about off-Facebook activity](#), how we use it and how you can manage it.

Everyone:

You can opt out of seeing online interest-based ads from Meta and other participating companies through the [Digital Advertising Alliance](#) in the US, the [Digital Advertising Alliance of Canada](#) in Canada or the [European Interactive Digital Advertising Alliance](#) in Europe or through your mobile device settings, where available, using Android, iOS 13 or an earlier version of iOS. Please note that ad blockers and tools that restrict our cookie use may interfere with these controls.

More information about online advertising:

The advertising companies we work with generally use cookies and similar technologies as part of their services. To learn more about how advertisers generally use cookies and the choices they offer, you can review the following resources:

- [Digital Advertising Alliance](#)
- [Digital Advertising Alliance of Canada](#)
- [European Interactive Digital Advertising Alliance](#)

Browser cookie controls:

In addition, your browser or device may offer settings that allow you to choose whether browser cookies are set and to delete them. These controls vary by browser, and manufacturers may change both the settings they make available and how they work at any time. As of 23 June 2021, you may find additional information about the controls offered by popular browsers at the links below. Certain parts of the Meta Products may not work properly if you have disabled browser cookie use. Please be aware that these controls are distinct from the controls that we offer you.

- [Google Chrome](#)
- [Internet Explorer](#)
- [Firefox](#)
- [Safari](#)
- [Safari Mobile](#)
- [Opera](#)

Date of last revision: 4 January 2022

English (US) Español Français (France) 中文(简体) العربية Português (Brasil) Italiano 한국어 Deutsch हिन्दी 日本語

[Sign Up](#) [Log In](#) [Messenger](#) [Facebook Lite](#) [Watch](#) [Places](#) [Games](#) [Marketplace](#) [Facebook Pay](#) [Oculus](#) [Portal](#) [Instagram](#) [Bulletin](#) [Local](#)
[Fundraisers](#) [Services](#) [Voting Information Center](#) [Groups](#) [About](#) [Create Ad](#) [Create Page](#) [Developers](#) [Careers](#) [Privacy](#) [Cookies](#) [Ad choices](#) [Terms](#)
[Help](#) [Contact](#) [Uploading & Non-Users](#)

Meta © 2022

Exhibit D

Our updated [Data Processing Terms](#) include a reference to our new [Data Transfer Addendum](#) incorporating Standard Contractual Clauses (replacing the Privacy Shield), effective August 31, 2020.

Facebook Business Tools Terms

When you use the [Facebook Business Tools](#) to send us or otherwise enable the collection of Business Tool Data (as defined in Section 1 below), these terms govern the use of that data.

Background: Ad Products and other Business Tools

We may receive Business Tool Data as a result of your use of Facebook ad products, in connection with advertising, matching, measurement and analytics. Those ad products include, but are not limited to, Facebook Pixel, Conversions API (formerly known as Server-Side API), Facebook SDK for App Events, Offline Conversions, App Events API and Offline Events API. We also receive Business Tools Data in the form of impression data sent by Facebook Social Plugins (for example the Like and Share buttons) and Facebook Login, and data from certain APIs such as Messenger Customer Match via the Send API. Facebook may also offer pilot, test, alpha, or beta programs from time to time through which you may provide Business Tool Data. Uses of Business Tools Data are described below.

By clicking "Accept" or using any of the Facebook Business Tools, you agree to the following:

1. [Sharing Business Tool Data with Facebook](#)

- a. You may use the Facebook Business Tools to send us one or both of the following types of personal information ("**Business Tool Data**") for the purposes described in Section 2:
 - i. "**Contact Information**" is information that personally identifies individuals, such as names, email addresses, and phone numbers, that we use for matching purposes only. We will hash Contact Information that you send to us via a Facebook JavaScript pixel for matching purposes prior to transmission. When using a Facebook image pixel or other Facebook Business Tools, you or your service provider must hash Contact Information in a manner specified by us before transmission.
 - ii. "**Event Data**" is other information that you share about people and the actions that they take on your websites and apps or in your shops, such as visits to your sites, installations of your apps, and purchases of your products. While Event Data does include information collected and transferred when people access a website or app with [Facebook Login](#) or [Social Plugins](#) (e.g. the Like button), it does not include information created when an individual interacts with our platform via Facebook Login, Social Plugins, or otherwise (e.g. by logging in, or liking or sharing an article or song). Information created when an individual interacts with our platform via Facebook Login, Social Plugins, or otherwise is governed by the [Platform Terms](#).
 - iii. Note: for purposes of these Business Tool Terms, references in existing terms or agreements to "Customer Data" will now mean "Business Tool Data."
- b. Subject to Section 1.d, we will not share Business Tool Data that you provide to us with third parties (including advertisers) unless you advise us that we are permitted to do so or we are required to do so by law.
- c. We will implement processes and procedures to protect the confidentiality and security of the Business Tool Data, including by maintaining appropriate organizational, technical and physical safeguards that are designed to (a) protect the security and integrity of the Business Tool Data while they are within our systems and (b) guard against the accidental or unauthorized access, use, alteration, or disclosure of Business Tool Data within our systems. These processes and procedures include the measures listed in Facebook's [Data Security Terms](#) (as updated from time to time, for example, to reflect technological developments) which are expressly incorporated into these Business Tools Terms.
- d. You agree that Facebook may provide access to and/or a copy of Event Data about a particular individual to that individual upon their request.
- e. You represent and warrant that you (and any data provider that you may use) have all of the necessary rights and permissions and a lawful basis (in compliance with all applicable laws, regulations and industry guidelines) for the disclosure and use of Business Tool Data.
- f. You will notify us promptly in writing of any actual or threatened complaint or challenge related to the use of any Business Tool Data under these Business Tools Terms and will cooperate with us in responding to such a complaint

or challenge.

- g. If you are using or sharing the Business Tool Data on behalf of or together with a third party, you also represent and warrant that you have the authority as agent to such third party to use, share, and process such data on its behalf and bind such third party to these Business Tools Terms. You will only use or share the Business Tool Data or any audience or reports generated through use of the Business Tool Data with or on behalf of such third party.
- h. You will not share Business Tool Data with us that you know or reasonably should know is from or about children under the age of 13 or that includes health, financial information or other categories of sensitive information (including any information defined as sensitive under applicable laws, regulations and applicable industry guidelines).

2. Use of Business Tool Data

- a. We will use Business Tool Data for the following purposes depending on which Facebook Business Tools you choose to use:
 - i. **Contact Information for Matching**
 - 1. You instruct us to process the Contact Information solely to match the Contact Information against user IDs ("**Matched User IDs**"), as well as to combine those user IDs with corresponding Event Data. We will delete Contact Information following the match process.
 - ii. **Event Data for Measurement and Analytics Services**
 - 1. You may instruct us to process Event Data (a) to prepare reports on your behalf on the impact of your advertising campaigns and other online content ("**Campaign Reports**") and (b) to generate analytics and insights about people and their use of your apps, websites, products and services ("**Analytics**").
 - 2. We grant to you a non-exclusive and non-transferable license to use the Campaign Reports and Analytics for your internal business purposes only and solely on an aggregated and anonymous basis for measurement purposes. You will not disclose the Campaign Reports or Analytics, or any portion thereof, to any third party, unless otherwise agreed to in writing by us. We will not disclose the Campaign Reports or Analytics, or any portion thereof, to any third party without your permission, unless (i) they have been combined with Campaigns Reports and Analytics from numerous other third parties and (ii) your identifying information is removed from the combined Campaign Reports and Analytics.
 - iii. **Event Data for Targeting Your Ads**
 - 1. You may provide Event Data to target your ad campaigns to people who interact with your business. You may direct us to create custom audiences, which are groups of Facebook users based on Event Data, to target ad campaigns (including Website Custom Audiences, Mobile App Custom Audiences, and Offline Custom Audiences). Facebook will process Event Data to create such audiences for you. You may not sell or transfer these audiences, or authorize any third party to sell or transfer these audiences. Facebook will not provide such audiences to other advertisers unless you or your service providers share audiences with other advertisers through tools we make available for that purpose, subject to the restrictions and requirements of those tools and our terms.
 - 2. These terms apply to the use of Website Custom Audiences, Mobile App Custom Audiences, and Offline Custom Audiences created through Facebook's Business Tools. Customer List Custom Audiences provided through our separate custom audience feature are subject to the Customer List Custom Audience Terms.
 - iv. **Event Data To Deliver Commercial and Transactional Messages**
 - 1. We may use the Matched User IDs and associated Event Data to help you reach people with transactional and other commercial messages on Messenger and other [Facebook Company Products](#).
 - v. **Event Data to Improve Ad Delivery, Personalize Features and Content and to Improve and Secure the Facebook Products**
 - 1. You may provide Event Data to improve ad targeting and delivery optimization of your ad campaigns. We may correlate that Event Data to people who use Facebook Company Products to support the objectives of your ad campaign, improve the effectiveness of ad delivery models, and determine the relevance of ads to people. We may use Event Data to personalize the features and content (including ads and recommendations) that we show people on and off our Facebook Company Products. In connection with ad

targeting and delivery optimization, we will: (i) use your Event Data for delivery optimization only after aggregating such Event Data with other data collected from other advertisers or otherwise collected on Facebook Products; and (ii) not allow other advertisers or third parties to target advertising solely on the basis of your Event Data.

2. To improve the experience for people who use Facebook Company Products, we may also use Event Data to promote safety and security on and off the Facebook Company Products, for research and development purposes and to maintain the integrity of and to improve the Facebook Company Products.

3. Special Provisions Concerning the Use of Certain Business Tools

- a. This section applies to your use of Business Tools to enable Facebook to store and access cookies or other information on an end user's device.
- b. You (or partners acting on your behalf) may not place pixels associated with your Business Manager or ad account on websites that you do not own without our written permission.
- c. You represent and warrant that you have provided robust and sufficiently prominent notice to users regarding the Business Tool Data collection, sharing and usage that includes, at a minimum:
 - i. For websites, a clear and prominent notice on each web page where our pixels are used that links to a clear explanation (a) that third parties, including Facebook, may use cookies, web beacons, and other storage technologies to collect or receive information from your websites and elsewhere on the Internet and use that information to provide measurement services and target ads, (b) how users can opt-out of the collection and use of information for ad targeting, and (c) where a user can access a mechanism for exercising such choice (e.g., providing links to: <http://www.aboutads.info/choices> and <http://www.youronlinechoices.eu/>).
 - ii. For apps, a clear and prominent link that is easily accessible inside your app settings or any privacy policy and from within any store or website where your app is distributed that links to a clear explanation (a) that third parties, including Facebook, may collect or receive information from your app and other apps and use that information to provide measurement services and targeted ads, and (b) how and where users can opt-out of the collection and use of information for ad targeting.
- d. In jurisdictions that require informed consent for storing and accessing cookies or other information on an end user's device (such as but not limited to the European Union), you must ensure, in a verifiable manner, that an end user provides all necessary consents before you use Facebook Business Tools to enable the storage of and access to Facebook cookies or other information on the end user's device. (For suggestions on implementing consent mechanisms, visit [Facebook's Cookie Consent Guide for Sites and Apps.](#))

4. Modification, Termination, and Retention:

- a. We may modify, suspend, or terminate your access to, or discontinue the availability of the Facebook Business Tools at any time. You may discontinue your use of the Facebook Business Tools at any time.
- b. Subject to these Business Tools Terms, we may retain the Event Data for a maximum of two years. We will retain any audiences you create using the Event Data until you delete them via your account tools. These Business Tools Terms do not replace any terms applicable to your purchase of advertising inventory from us (including but not limited to the [Self-Serve Ad Terms](#) and the [Facebook Advertising Policies](#)) and such terms will continue to apply to your ad campaigns. [Facebook's Custom Audience Terms](#) will not apply to audiences generated through the processing of Business Tools Data under these Business Tools Terms.
- c. We reserve the right to monitor or audit your compliance with these Business Tools Terms.
- d. These terms supplement and amend the [Facebook Commercial Terms of Service](#). Facebook may update these Business Tools Terms from time to time. By continuing to access or use the Business Tools after any update, you agree to be bound by it. The parties acknowledge and agree that the US [State-Specific Terms](#) may apply to the provision and use of the Facebook Business Tools and are incorporated into these Business Tools Terms by reference.
- e. Nothing in these Business Tools Terms will prevent us from making disclosures to our users in relation to Facebook Business Tools as we may be advised or as we may determine are appropriate or required under applicable law.
- f. In the event of any express conflict between these Business Tools Terms and the Commercial Terms, these Business Tools Terms will govern solely with respect to your use of the Facebook Business Tools, and solely to the extent of the conflict.

5. Additional Terms for Processing of Personal Information

- a. To the extent the Business Tool Data contain Personal Information which you Process subject to the General Data Protection Regulation (Regulation (EU) 2016/679) (the “GDPR”), the following terms apply:
 - i. The parties acknowledge and agree that you are the Controller in respect of the Processing of Personal Information in Business Tool Data for purposes of providing matching, measurement and analytics services described in Sections 2.a.i and 2.a.ii above (e.g. to provide you with Analytics and Campaign Reports), and that you instruct Facebook Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2 Ireland (“Facebook Ireland”) to Process such Personal Information for those purposes on your behalf as your Processor pursuant to these Business Tools Terms and Facebook’s [Data Processing Terms](#). The [Data Processing Terms](#) are expressly incorporated herein by reference and apply between you and Facebook Ireland together with these Business Tools Terms.
 - ii. Regarding Personal Information in Event Data referring to people’s actions on your websites and apps which integrate Facebook Business Tools for whose Processing you and Facebook Ireland jointly determine the means and purposes, you and Facebook Ireland acknowledge and agree to be Joint Controllers in accordance with Article 26 GDPR. The joint controllership extends to the collection of such Personal Information via the Facebook Business Tools and its subsequent transmission to Facebook Ireland in order to be used for the purposes set out above under Sections 2.a.iii to 2.a.v.1 (“Joint Processing”). For further information, click [here](#). The Joint Processing is subject to the [Controller Addendum](#), which is expressly incorporated herein by reference and applies between you and Facebook Ireland together with these Business Tools Terms. Facebook Ireland remains an independent Controller in accordance with Article 4(7) GDPR for any Processing of such data that takes place after it has been transmitted to Facebook Ireland.
 - iii. You, as the case may be, and Facebook Ireland remain independent Controllers in accordance with Article 4(7) GDPR for any Processing of Personal Information in Business Tool Data under GDPR not subject to Sections 5.a.i and 5.a.ii.
- b. Section 5.a.i also applies when you are in Andorra, Azores, Canary Islands, Channel Islands, French Guiana, Guadeloupe, Isle of Man, Madeira, Martinique, Mayotte, Monaco, Réunion, San Marino, Saint Barthélemy, Saint-Martin, Switzerland, United Kingdom sovereign bases in Cyprus (Akrotiri and Dhekelia), and Vatican City.
- c. To the extent the Business Tool Data contain Personal Information which you Process not subject to GDPR and you are not in any of the territories listed in Section 5.b, you acknowledge and agree that you are the Controller in respect of the Processing of such Personal Information for purposes of providing matching, measurement and analytics services described in Sections 2.a.i and 2.a.ii above (e.g. to provide you with Analytics and Campaign Reports), and you instruct Facebook, Inc., 1 Hacker Way, Menlo Park, CA 94025, USA to Process such Personal Information for those purposes on your behalf as your Processor pursuant to these Business Tools Terms and Facebook’s [Data Processing Terms](#). The [Data Processing Terms](#) are expressly incorporated herein by reference and apply in addition to these Business Tools Terms.
- d. “Personal Information”, “Controller”, “Processor” and “Processing” in this Section have the meanings set out in the [Data Processing Terms](#). References to GDPR and its provisions in this Section 5 include the GDPR as amended and incorporated into UK law after the GDPR ceases to apply in the UK.

Note:

- i. We have updated the Terms For Conversion Tracking, Custom Audiences From Your Website, and Custom Audiences From Your Mobile App, including changing its name to the [Facebook Business Tools Terms](#). For purposes of the Facebook Business Tools Terms, references in existing terms or agreements to the “Facebook Tools” will now mean Facebook Business Tools.
- ii. We have updated the Offline Conversion Terms, including changing its name to the Facebook Business Tools Terms. For the purposes of the Facebook Business Tools Terms, references in existing terms or agreements to (i) “Sales Data” will now mean Business Tool Data; (ii) “User Information” will now mean Contact Information; (iii) “Sales Transaction Data” will now mean Event Data; (iv) “Matched Data” will now mean Event Data that is combined with Matched User IDs; (v) “Unmatched Data” will now mean Event Data that is not combined with Matched User IDs; (vi) “Reports” will now mean Campaign Reports; and (vii) “OC” will now mean our Offline Conversions feature.

Effective date: August 31, 2020

Exhibit E

[Log In](#)

The Facebook company is now Meta. We've updated our Terms of Use, Data Policy, and Cookies Policy to reflect the new name on January 4, 2022. While our company name has changed, we are continuing to offer the same products, including the Facebook app from Meta. Our Data Policy and Terms of Service remain in effect, and this name change does not affect how we use or share data. [Learn more about Meta](#) and our vision for the metaverse.

These terms reflect our updated [European Data Transfer Addendum](#) incorporating new Standard Contractual Clauses effective September 27, 2021.

Meta Commercial Terms ("Commercial Terms")

These Commercial Terms apply to access or use of the [Meta Products](#) (or "Products"), for a business or commercial purpose (except where we state that separate terms, and not these Commercial Terms, apply to such access or use of a Facebook Product). Business or commercial purposes include using ads, selling products, developing apps, managing a Page, managing a Group for business purposes, or using our measurement services regardless of the entity type.

You agree that you will ensure that any third party on whose behalf you access or use any Meta Product for any business or commercial purpose will abide by the applicable terms of use, including these Commercial Terms, the [Meta Terms of Service](#) ("Terms"), and any applicable supplemental terms, and you represent and warrant that you have the authority to bind that third party to such terms.

As more fully described below, if you reside in the United States or your business is located in the United States, these Commercial Terms require the resolution of most disputes between you and us by binding arbitration on an individual basis; class actions and jury trials are not permitted.

Licenses: As described in "[The permissions you give us](#)" section in our Terms, you grant us a license to content that is covered by intellectual property rights (like photos or videos) you share, post, or upload on or in connection with our Meta Products. For any access or use of the Meta Products, that license applies to content you or someone on your behalf (such as your agency that places an ad for you or your service provider that manages your Page content for you) makes available on or in connection with any Meta Product. You also will ensure that you own or have secured all rights necessary to grant the licenses and rights you (or someone on your behalf) grant to us under the Commercial Terms and any applicable supplemental terms, including permission to display, distribute and deliver your content within the Meta Products.

Compliance with Law: You represent and warrant that your access or use of the Meta Products for business or commercial purposes complies with all applicable laws, rules, and regulations. You further represent that you will restrict access to your content and apps in accordance with all applicable laws, rules, and regulations, including geo-filtering or age-gating access where required. In addition to and without limiting the requirements about who can use the Meta Products under our Terms, if you are located in a country that is subject to embargo under the laws of the United States (or under similar laws applicable to you) you may not engage in commercial activities on the Meta Products unless authorized by applicable laws. If you are on the U.S. Treasury Department's list of Specially Designated Nationals (or an equivalent list), you may not engage in commercial or business activities on the Meta Products (such as advertising or payments). You also may not access or use the Meta Products if you are prohibited from receiving products, services, or software under applicable law.

Data Restrictions: You may not send us information prohibited by the supplemental terms or policies. In addition, you may not send to us, or use Meta Products to collect from people, information that: (i) you know or reasonably should know is from or about children under the age of 13; or (ii) includes health, financial, biometrics, or other categories of similarly sensitive information (including any information defined as sensitive under applicable law); except in cases where (a) the terms for that Meta Product specifically allow it or (b) you are sending financial information for the express purpose of effecting a financial transaction either with us or as enabled by a Meta Product.

Limits on Liability: In addition to and without limiting the scope of the “*Limits on liability*” section in our Terms, you agree that we are not responsible for the actions, services, content, or data of third parties and you release us, our directors, officers, employees, and agents from any claims and damages, known or unknown, arising out of or in any way connected with any claim you have against any such third parties.

If you are a California resident, you agree to waive California Civil Code § 1542, which says:

A GENERAL RELEASE DOES NOT EXTEND TO CLAIMS WHICH THE CREDITOR DOES NOT KNOW OR SUSPECT TO EXIST IN HIS OR HER FAVOR AT THE TIME OF EXECUTING THE RELEASE, WHICH IF KNOWN BY HIM OR HER MUST HAVE MATERIALLY AFFECTED HIS OR HER SETTLEMENT WITH THE DEBTOR.

Our aggregate liability arising out of or relating to any access or use of the Meta Products, the Terms (for any access or use of the Meta Products for business or commercial purposes), or these Commercial Terms will not exceed the greater of one hundred dollars (\$100) or the amount you have paid us in the past twelve months.

Disputes:

Third Party Claims: If anyone brings a claim, cause of action, or dispute against us related to your services, actions, content or information on Facebook or other Meta Products or your use of any Meta Products, you agree to indemnify and hold us harmless from and against any damages, losses, and expenses of any kind (including reasonable legal fees and costs) related to any such claim, cause of action, or dispute.

Commercial Claims: Sections 5.c and 5.d below apply to any claim, cause of action, or dispute that arises out of or relates to any access or use of the Meta Products for business or commercial purposes (“Commercial Claim”) between you and Meta.

U.S. Commercial Claims: If you reside in the United States or your business is located in the United States:

You agree to arbitrate Commercial Claims between you and Meta Platforms, Inc. This provision does not cover any commercial claims relating to violations of your or our intellectual property rights, including, but not limited to, copyright infringement, patent infringement, trademark infringement, violations of the [Brand Usage Guidelines](#), violations of your or our confidential information or trade secrets, or efforts to interfere with our Products or engage with our Products in unauthorized ways (for example, automated ways). If a Commercial Claim between you and Meta Platforms, Inc. is not subject to arbitration, you agree that the claim must be resolved exclusively in the U.S. District Court for the Northern District of California or a state court located in San Mateo County, and that you submit to the personal jurisdiction of either of these courts for the purpose of litigating any such claim.

We and you agree that, by entering into this arbitration provision, all parties are waiving their respective rights to a trial by jury or to participate in a class or representative action. THE PARTIES AGREE THAT EACH MAY BRING COMMERCIAL CLAIMS AGAINST THE OTHER ONLY IN ITS INDIVIDUAL CAPACITY, AND NOT AS A PLAINTIFF OR CLASS MEMBER IN ANY PURPORTED CLASS, REPRESENTATIVE, OR PRIVATE ATTORNEY GENERAL PROCEEDING. You may bring a Commercial Claim only on your own behalf and cannot seek relief that would affect other parties. If there is a final judicial determination that any particular Commercial Claim (or a request for particular relief) cannot be arbitrated according to the limitations of this Section 5.c, then only that Commercial Claim (or only that request for relief) may be brought in court. All other Commercial Claims (or requests for relief) will remain subject to this Section 5.c. The Federal Arbitration Act governs the interpretation and enforcement of this arbitration provision. All issues are for an arbitrator to decide, except that only a court may decide issues relating to the scope or enforceability of this arbitration provision or the interpretation of the prohibition of class and representative actions. If any party intends to seek arbitration of a dispute, that party must provide the other party with notice in writing. This notice of dispute to us must be sent to the following address: Meta Platforms, Inc. 1601 Willow Rd. Menlo Park, CA 94025. The arbitration will be governed by the AAA's Commercial Arbitration Rules ("AAA Rules"), as modified by these Commercial Terms, and will be administered by the AAA. If the AAA is unavailable, the parties will agree to another arbitration provider or the court will appoint a substitute. The arbitrator will not be bound by rulings in other arbitrations in which you are not a party. To the fullest extent permitted by applicable law, any evidentiary submissions made in arbitration will be maintained as confidential in the absence of good cause for its disclosure. The arbitrator's award will be maintained as confidential only to the extent necessary to protect either party's trade secrets or proprietary business information or to comply with a legal requirement mandating confidentiality. Each party will be responsible for paying any AAA filing, administrative and arbitrator fees in accordance with AAA Rules, except that we will pay for your filing, administrative, and arbitrator fees if your Commercial Claim for damages does not exceed \$75,000 and is non-frivolous (as measured by the standards set forth in Federal Rule of Civil Procedure 11(b)). If you do not wish to be bound by this provision (including its waiver of class and representative claims), you must notify us as set forth below within 30 days of the first acceptance date of any version of these Commercial Terms containing an arbitration provision. Your notice to us under this Section 5.c must be submitted to the address here: Meta Platforms, Inc. 1601 Willow Rd. Menlo Park, CA 94025. All Commercial Claims between us, whether subject to arbitration or not, will be governed by California law, excluding California's conflict of laws rules, except to the extent that California law is contrary to or preempted by federal law. If a Commercial Claim between you and us is not subject to arbitration, you agree that the claim must be resolved exclusively in the U.S. District Court for the Northern District of California or a state court located in San Mateo County, and that you submit to the personal jurisdiction of either of these courts for the purpose of litigating any such claim.

Commercial Claims outside the United States: If you reside outside the United States or your business is located outside the United States, you agree that:

Any Commercial Claim between you and Meta Platforms, Inc. must be resolved exclusively in the U.S. District Court for the Northern District of California or a state court located in San Mateo County, that you submit to the personal jurisdiction of either of these courts for the purpose of litigating any such claim, and that the laws of the State of California will govern these Commercial Terms and any such claim, without regard to conflict of law provisions.

Any Commercial Claim between you and Meta Platforms Ireland Limited must be resolved

exclusively in the courts of the Republic of Ireland, that you submit to the personal jurisdiction of the Republic of Ireland for the purpose of litigating any such claim, and the laws of the Republic of Ireland will govern these Commercial Terms and any such claim, without regard to conflict of law provisions.

Notwithstanding (i) and (ii) above, any Commercial Claim between you and both Meta Platforms, Inc. and Meta Platforms Ireland Limited must be resolved exclusively in the U.S. District Court for the Northern District of California or a state court located in San Mateo County, that you submit to the personal jurisdiction of either of these courts for the purpose of litigating any such claim, and that the laws of the State of California will govern these Commercial Terms and any such claim, without regard to conflict of law provisions.

Without prejudice to the foregoing, you agree that, in our sole discretion, we may also bring any claim we have against you related to efforts to abuse, interfere, or engage with our Products in unauthorized ways in the country in which you reside that has jurisdiction over the claim.

Severability: If any provision of this Section 5 is found unenforceable, that provision will be severed and the balance of this Section 5 will remain in full force and effect.

Updates: We may need to update these Commercial Terms from time to time, including to accurately reflect the access or uses of our Products for business or commercial purposes, and so we encourage you to check them regularly for any updates. By continuing any access or use of any Meta Products for business or commercial purposes after any notice of an update to these Commercial Terms, you agree to be bound by them. Any updates to Section 5 of these Commercial Terms will apply only to disputes that arise after notice of the update takes place. If you do not agree to the updated terms, please stop all access or use of our Products for business or commercial purposes.

Conflicts and Supplemental Terms: If there is a conflict between these Commercial Terms and the Terms, these Commercial Terms will govern with respect to your access and use of the Meta Products for business or commercial purposes to the extent of the conflict. Supplemental terms and policies may also apply to your use of certain Meta Products. To the extent those supplemental terms conflict with the Commercial Terms, the supplemental terms will govern with respect to your use of those Meta Products to the extent of the conflict.

If any portion of these Commercial Terms are found to be unenforceable, then (except as otherwise provided) that portion will be severed and the remaining portion will remain in full force and effect.

If we fail to enforce any of these Commercial Terms, it will not be considered a waiver.

Except as permitted in Section 6, any amendment to or waiver of these Commercial Terms must be made in writing and signed by us.

You will not transfer any of your rights or obligations under these Commercial Terms to anyone else without our consent.

These Commercial Terms do not confer any third party beneficiary rights.

We offer tools to provide transparency and controls to our users about the Facebook experience,

including information to show them why they are being shown specific content or provide feedback about content, and controls to block content or stop seeing certain types of content (such as by removing themselves from interests used for advertising). You agree that information about you and your use of Meta Products for commercial or business purposes may be included in these tools. For clarity, our license to content extends to the display of content in conjunction with providing these tools.

You consent that we may disclose your advertising content and Facebook Page posts (“Commercial Content”), and all information associated with such Commercial Content, including information associated with the delivery of that Commercial Content, in response to valid legal process related to an electoral matter or to a governmental entity or body if Meta believes that disclosure would assist in a lawful investigation.

Please note that our retention policies for Commercial Content may differ from those set forth in the Terms. We retain Commercial Content as necessary to provide our services to users, for internal record keeping, and for product improvement and safety purposes.

All of our rights and obligations under these Commercial Terms are freely assignable by us in connection with a merger, acquisition, or sale of assets, or by operation of law or otherwise.

Nothing in these Commercial Terms or any applicable supplemental terms will prevent us from complying with the law.

We reserve all rights not expressly granted to you.

Note: For purposes of these Commercial Terms, references in existing terms or agreements to (i) “the Statement of Rights and Responsibilities,” “Statement,” or “SRR,” will now mean the Meta Terms or Terms and (ii) “Facebook” (when used to refer to our products and services) or “Facebook Services” or “Services” will now mean Meta Products.

Effective Date: January 4, 2022


[English \(US\)](#) [Español](#) [Français \(France\)](#) [中文\(简体\)](#) [العربية](#) [Português \(Brasil\)](#) [Italiano](#) [한국어](#) [Deutsch](#) [हिन्दी](#) [日本語](#)



[Sign Up](#) [Log In](#) [Messenger](#) [Facebook Lite](#) [Watch](#) [Places](#) [Games](#) [Marketplace](#) [Meta Pay](#) [Oculus](#) [Portal](#) [Instagram](#) [Bulletin](#) [Local](#)
[Fundraisers](#) [Services](#) [Voting Information Center](#) [Groups](#)


[Privacy](#) · [Terms](#) · [Advertising](#) · [Ad Choices](#)  · [Cookies](#) · [More](#) · Meta © 2022

Exhibit F



Off-Facebook activity

Off-Facebook activity includes information that businesses and organizations share with us about your interactions with them, such as visiting their apps or websites.




What is off-Facebook activity?

>


What you can do

You can control or disconnect the information businesses send to Facebook.




Recent activity
Spotify: Music and Podcasts, Hopper: Hotels, Flights & Cars, and more

>




Explore activity

>



Clear previous activity

>



Disconnect future activity

>

Exhibit G

- Using Facebook
- Managing Your Account
- Privacy, Safety and Security
- Policies and Reporting

How do I disconnect my off-Facebook activity?

Computer Help

Copy link

You can disconnect your past off-Facebook activity from your account with the clear history control in your off-Facebook activity setting.

Off-Facebook activity is a summary of activity that businesses and organizations share with us about your interactions with them, such as visiting their apps or websites. They use our [Business Tools](#), like Facebook Login or Facebook Pixel, to share this information with us. This helps us do things like give you a more personalized experience on Facebook. Learn more [about off-Facebook activity](#) and how we use it.

To disconnect your off-Facebook activity from your account:

1. Click your profile picture in the top right of Facebook.
2. Select **Settings & privacy**, then click **Settings**.
3. Click **Privacy** in the left menu.
4. Click **Your Facebook information**, then click **Off-Facebook activity**.
5. Click **Clear previous activity**, then click **Clear previous activity**.

You can also choose to turn off your future off-Facebook activity. Learn more [about managing your future activity](#).

When you disconnect your off-Facebook activity from your account:

- Only your off-Facebook activity history will be disconnected from your account.
- Disconnecting your history may log you out of apps and websites. If this happens, you can still use Facebook to log back in.
- You may still see ads from these businesses. For example, advertisers can show ads based on your activity on Facebook, such as when you like a business page. Also, they can upload lists and show their ads to people on that list. Learn more about advertisers using these lists on your [Ad Preferences](#) page.
- You'll still see the same number of ads, but the ads you see may be less personalized to you.

Other ways you can manage your Facebook experience:

You can take more control over what information you see in your Feed, ads and other parts of Facebook without disconnecting your off-Facebook activity. Here are a few ways to control your Facebook experience:

- Update your [Feed preferences](#) to see more content on your Feed that you're interested in.
- Customize your [Ad Preferences](#) to see ads that are more relevant to you. From here, you can [update your ad settings](#) to control things like if we show you ads based on your use of apps and websites off Facebook.
- You can also [hide an ad](#) that isn't interesting or useful to you or [review why you're seeing a particular ad](#).
- Walk through [Privacy Checkup](#) to make sure you're sharing your information with who you want.
- Visit [Access Your Information](#) to see and manage your Facebook information, or [download your Facebook information](#) for review.

Related Articles

- [Find your Facebook activity log](#)
- [How do I manage my future off-Facebook activity?](#)
- [What's included in my Facebook activity log?](#)
- [Turn your active status on or off on Facebook](#)
- [How do I temporarily deactivate my Facebook account?](#)

Exhibit H

- Using Facebook
- Managing Your Account
- Privacy, Safety and Security
- Policies and Reporting

How do I manage my future off-Facebook activity?

Computer Help

Copy link

You can choose to turn off your future off-Facebook activity with the **Manage Future Activity** setting.

Off-Facebook activity is a summary of activity that businesses and organizations share with us about your interactions with them, such as visiting their apps or websites. They use our [Business Tools](#), like Facebook Login or Facebook Pixel, to share this information with us. This helps us do things like give you a more personalized experience on Facebook. Learn more [about off-Facebook activity](#) and how we use it.

You can also choose to [disconnect your off-Facebook activity](#), which will disconnect your past activity from your account. Keep in mind, when you turn off future activity for all apps and websites, it'll also disconnect your past activity.

To turn off your future off-Facebook activity for all apps and websites:

1. Click your profile picture in the top right of Facebook.
2. Select **Settings & privacy**, then click **Settings**.
3. Click **Your Facebook Information** in the left column, then click **Off-Facebook Activity**.
4. Click **Manage Your Off-Facebook Activity**, then click **Manage Future Activity**.
5. Click **Manage Future Activity**.
6. Click next to **Future Off-Facebook Activity**, then click **Turn Off** to turn off your future off-Facebook activity.

To turn off your future off-Facebook activity for one app or website:

1. Click your profile picture in the top right of Facebook.
2. Select **Settings & privacy**, then click **Settings**.
3. Click **Your Facebook Information** in the left column, then click **Off-Facebook Activity**.
4. Click **Manage Your Off-Facebook Activity**. You'll be prompted to re-enter your password.
5. Click the app or website you'd like to review.
6. Click **Turn off future activity from [name of business or organization]**, then click **Turn Off**.

When you turn off your future off-Facebook activity:

- Your future off-Facebook activity will be disconnected within 48 hours from when it's received. During this time it may be used for measurement purposes and to make improvements to our ads systems.
- If you choose to turn off your future activity for all apps and websites, you'll also disconnect all your past off-Facebook activity.
- You may still see ads from these businesses. For example, advertisers can show ads based on your activity on Facebook, such as when you like a business page. Also, they can upload customer lists and show their ads to people on that list. Learn more about advertisers using these lists on your [Ad Preferences](#) page.
- You'll still see the same number of ads, but the ads you see may be less personalized to you.
- You may be logged out of apps and websites. To log in with Facebook in the future, you'll have to allow information from that app or website to stay connected to your Facebook account.

Other ways you can manage your Facebook experience:

You can take more control over your information without turning off your off-Facebook activity. Here are a few ways to control your Facebook experience:

- Update your [Feed preferences](#) to see more content on your Feed that you're interested in.
- Customize your [Ad Preferences](#) to see ads that are more relevant to you. From here, you can [update your ad settings](#) to control things like if we show you ads based on your use of apps and websites off Facebook.
- You can also [hide an ad](#) that isn't interesting or useful to you or [review why you're seeing a particular ad](#).
- Walk through [Privacy Checkup](#) to make sure you're sharing your information with who you want.
- Visit [Access Your Information](#) to see and manage your Facebook information, or [download your Facebook information](#) for review.

Related Articles

- [Find your Facebook activity log](#)
- [How do I disconnect my off-Facebook activity?](#)
- [Turn your active status on or off on Facebook](#)
- [What's included in my Facebook activity log?](#)
- [Review your Off-Facebook activity](#)

Exhibit I

Ad Preferences

Advertisers

Ad Topics

Ad Settings

Data about your activity from partners

Personalized ads based on your activity on other websites, apps or offline



To show you relevant ads, we use data that advertisers and other [partners](#) provide to us about your activity on their websites and apps, as well as certain offline interactions, such as purchases. For example, we may show you an ad for a shirt based on your visit to a clothing website. We never sell your data. [Learn More](#)

Choose where we can use data from our partners to show you personalized ads.

Ad Preferences



Advertisers



Ad Topics



Ad Settings

Choose where we can use data from our partners to show you personalized ads.



Nealofar Panjshiri

Facebook



npanjshiri

Instagram



What You Should Know

This setting doesn't change the number of ads you'll see.



This setting controls how certain data is used.



Where this setting applies:



Was this section useful?

Yes

No



Social interactions

Who can see your social interactions alongside ads?

Exhibit J



Privacy Policy

Explore the policy

- What is the Privacy Policy and what does it cover? ✓
- What information do we collect? ✓
- How do we use your information? ✓
- How is your information shared on Meta Products or with Integrated Partners? ✓
- How do we share information with Partners, vendors, service providers and third parties? ✓
- How do the Meta Companies work together? ✓
- How can you manage or delete your information and exercise your rights? ✓
- How long do we keep your information? ✓
- How do we transfer information? ✓
- How do we respond to legal requests, comply with applicable law and prevent harm? ✓
- How will you know the policy has changed? ✓
- Privacy notice for California residents ✓
- How to contact Meta with questions ✓
- Why and how we process your information ✓

Other policies

- Terms of Service 
- Cookies Policy 

What is the Privacy Policy and what does it cover?

Effective July 26, 2022

We at Meta want you to understand what information we collect, and how we use and share it. That's why we encourage you to read our Privacy Policy. This helps you use Meta Products in the way that's right for you.

In the Privacy Policy, we explain how we collect, use, share, retain and transfer information. We also let you know your rights. Each section of the Policy includes helpful examples and simpler language to make our practices easier to understand. We've also added links to resources where you can learn more about the privacy topics that interest you.

It's important to us that you know how to control your privacy, so we also show you where you can manage your information in the settings of the Meta Products you use. You can [update these settings](#) to shape your experience.

Read the full policy below.

What Products does this policy cover? ^[1]



Learn more in Privacy Center about managing your privacy



1

What Products does this policy cover?

This policy describes the information we, Meta Platforms, Inc., process to provide Meta Products. Meta Products, which we also call "Products," include:







- Facebook
- Messenger
- Instagram (including apps like Boomerang)
- Facebook Portal products
- [Meta Platforms Technologies Products](#) (when linked to a Facebook account)
- Shops
- Marketplace
- Spark AR
- Meta Business Tools
- Meta Audience Network
- [NPE Team apps](#)

- Facebook View

Some of our Products also have a [supplemental privacy policy^{\[2\]}](#) that adds to the information provided in this policy.

2

Supplemental policies

Bulletin	
Facebook Portal products	
Facebook View	
Free Basics	
Oculus Products	
Oversight Board	

What information do we collect?

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^{\[3\]}](#).

Here's the information we collect:

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](#)^[4], such as:

- Content you create, like posts, comments or [audio](#)^[5]
- Content you provide through our camera feature or your camera roll settings, or through our voice-enabled features. [Learn more](#)^[6] 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](#)^[7] about content and messages, subject to applicable law
- Types of content 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](#)^[8].
- Purchases or other transactions you make, including credit card information. [Learn more](#)^[9].
- 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, political views, who you are "interested in" (which could reveal your sexual orientation) or your health in your Facebook [profile fields](#) or life events. This and other infor-

mation (such as racial or ethnic origin, philosophical beliefs or trade union membership) could have special protections under the laws of your country.

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](#)^[10].

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.

App, browser and device information

We collect and receive information from and about the different [devices](#)^[11] you use and how you use them.

Device information we collect and receive includes:

- The device and software you're using, and other device characteristics. [See examples](#)^[12].

- What you're doing on your device, like whether our app is in the foreground or if your mouse is moving (which can help tell humans from bots)
- Identifiers that tell your device apart from other users', including Family Device IDs. [See examples^{\[13\]}](#).
- Signals from your device. [See examples^{\[14\]}](#).
- Information you've shared with us through device settings, like GPS location, camera access, photos and [related metadata^{\[15\]}](#)
- Information about the network you connect your device to, including your IP address. [See more examples^{\[16\]}](#).
- Information about our Products' performance on your device. [Learn more^{\[17\]}](#).
- Information from cookies and similar technologies. [Learn more.^{\[18\]}](#)

Information from Partners, vendors and third parties

What kinds of information do we collect or receive?

We collect and receive information from [Partners^{\[19\]}](#), [measurement vendors](#) and [third parties^{\[20\]}](#) 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
- 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^{\[18\]}](#) 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



Off-Facebook activity



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.

What if you don't let us collect certain information?

Some information is required for our Products to work. Other information is optional, but without it, the quality of your experience might be affected.

[Learn more](#)^[21] >

Take control in Privacy Center



Manage the information we collect about you



3

Information we collect if you use our Products but don't have an account

For example, we collect:

- Browser and app logs of your visits to public content, like Facebook Pages, videos and [rooms](#)

- Basic information about devices that downloaded our apps, like device model and OS

We also receive information using cookies and similar technologies, like the Meta Pixel or Social Plugins, when you visit other websites and apps that use Meta Products. Read our [Cookies Policy](#) to learn more.

Examples of why we collect information

Security of our Products

For example, if we see someone without an account trying to load too many pages, they could be trying to [scrape](#) our site in violation of our terms. Then we can take action to prevent it.

Safety and integrity

For example, if someone without an account joins a room and shares a harmful video, we can take action according to our Community Standards. We can remove content that violates our terms and policies, or share information with law enforcement when we believe there is a genuine risk of death or imminent bodily harm.

Advertising

For example, you may also see ads for the Meta Company Products shown through [Meta Audience Network](#) when you visit other apps if we can't recognize you as a registered user of the Meta Products.

Performance

For example, we use information we have about people who use our Products, even if they don't have an account, to measure how fast our pages load in different countries. This helps us identify and fix issues with local networks.

4

Information you provide

For example, when you create a Facebook account, you must provide some information, like a password and your email address or phone number. You might choose to add other details to your account, like a profile photo or payment information.

We also collect information you provide when you:

- Create your avatar

- Fill out a form
- Contact us

5

Audio content you create

You can create audio content, like if you're a host or speaker in a Live Audio Room. Live Audio can be listened to by anyone in the audience for the broadcast.

6

What we collect from our camera feature



José likes using Instagram's Camera feature to take pictures of his friends. We collect information about how José uses the Camera feature, including what he sees through the camera lens on his device while he's using the feature. This helps us do things like suggest masks and filters that he might like.

How filters, effects, masks and avatars work



If you use our camera or allow access to photos and videos, on certain Meta Products you can add filters, effects, masks or avatars. Some of these features process parts of faces or bodies within the camera frame, photo or video. Then they can do things like fit a mask correctly over the eyes, nose and mouth. The information we use for this process is used to create the feature. It's not used to identify you.

What we collect from voice-enabled features



Ren tells Meta's voice-enabled Assistant to take a photo on Ray-Ban Stories. A visual indicator shows that Assistant is activated and listening for Ren's command. We collect this voice interaction, which includes any background sound that occurs when Ren says the command. Collecting Ren's voice interactions lets us provide and, depending on Ren's settings, improve the Assistant feature.

Metadata is:

- 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

8

Apps and features you use, and how you use them

For example, we log:

- What apps, posts, videos, ads, games, Shops and other content you view or interact with on our Products
- When you use [Social Plugins](#), [Facebook Login](#) or autofill

9

Purchases or other transactions

We collect information when you use our Products to buy or sell things or make other financial transactions.

Some examples are:

- Purchases within an online game
- Donations to a friend's fundraiser
- Purchases in Marketplace, Shops or groups
- Money transfers to friends and family (where available)

What we collect from transactions

When you buy things or make other payments in Marketplace, Shops or groups, we collect information about your purchase or other financial transactions, like:

- Credit or debit card number and other card information
- Billing, shipping and contact details

- Items you bought and how many
- Other account and authentication information

Why we collect this information

One reason we store this information is to allow you to access and view your payment and transaction history.

And you can use it the next time you shop to give you easier, faster shopping experiences.

More in the Privacy Policy

How do we use your information?



How do we respond to legal requests, comply with applicable law and prevent harm?



10

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

11

Devices

These devices include computers, phones, hardware, connected TVs, Portal devices and other web-connected devices.

12

What device you're using, and other device characteristics

We collect device information like:

- The type of device
- Details about its operating system
- Details about its hardware and software
- Battery level
- Signal strength
- Available storage
- Browser type
- App and file names and types
- Plugins

13

Identifiers that tell your device apart from other users'

Identifiers we collect include device IDs, mobile advertiser ID or IDs from games, apps or accounts you use. We also collect Family Device IDs or other identifiers unique to [Meta Company Products](#) associated with the same device or account.

14

Device signals

Device signals include GPS, Bluetooth signals, nearby Wi-Fi access points, beacons and cell towers.

15

Related metadata

For example, if you give us permission to access your device's camera roll, we collect metadata. This metadata is from and about your photos and videos and includes the date and time they were made. We use this to do things like remind you when you have new photos to upload.

16

Information about the network you connect your device to

Information about your network includes:

- The name of your mobile operator or internet service provider (ISP)
- Language
- Time zone
- Mobile phone number
- IP address
- Connection speed
- Information about other devices that are nearby or on your network
- Wi-Fi hotspots you connect to using our Products

One reason we collect this information is to make your experience better. For example, if we know that your phone and TV are connected to the same network, we can help you use your phone to control a video stream on your TV.

More in the Privacy Policy

How do we use your information?



17

Information about our Products' performance on your device

We collect device information to prevent, diagnose, troubleshoot and fix errors and bugs. This includes how long the app was running, what model of device you were using and other performance and diagnostic information.

18

Cookies

Cookies are small pieces of text used to store information on web browsers. We use cookies and similar technologies, including data that we store on your web browser or device, identifiers associated with your device and other software, Social Plugins and the Meta Pixel. They help us provide, protect and improve our Products, such as by personalizing content, tailoring and measuring ads and providing a safer experience.

We collect information from cookies stored on your device, including cookie IDs and settings. Read our cookie policies:

- [Facebook Cookies Policy](#)
- [Instagram Cookies Policy](#)

19

Our Partners

Businesses and people can use our Products to advertise, market or support their products and services. When they use our Products, we call them our Partners.

Our Products include our Business Tools and other technologies that allow businesses to advertise or support their products and services, or to understand and measure how people are using their services and how well their ads are working. For example, they might put one of our Business Tools, the Meta Pixel, on their website. Or they might use Meta Audience Network tools to monetize their apps by showing ads from businesses that advertise on Facebook.

Our Products also include technologies where you can make a connection to our Partners through our Products. For example, you might log into their app or website using Facebook Login. Or you might play their game on Facebook, which we call an integration because you can play without leaving our app. We call the Partners who use these integrated tools our Integrated Partners.

Here are some examples of our Partners:

- Advertisers
- Companies that measure how well ads are doing and provide reports

- Businesses and people that use our Products to sell or offer goods and services
- Publishers (like a website or app) and their business partners
- App developers
- Game developers

20

Third parties we get information from

Other organizations and bodies share information with Meta but don't use our Products. We refer to them as third parties. We collect and receive information from these 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
- 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, such as translations
- Support AI research, like computer vision and natural language processing technologies

- Engage with research survey respondents who choose to participate in additional conversations

More in the Privacy Policy

How do we use your information?



21

What happens if you don't let us collect certain information

For example, if you don't provide an email address or phone number, we won't be able to create an account for you to use our Products.

Or you can choose not to add Facebook friends, but then your Facebook Feed won't show friends' photos and status updates.

How do we use your information?

We use [information we collect](#) to provide a personalized experience to you, including ads, along with the other purposes we explain in detail below.

For some of these purposes, we use information [across our Products](#)^[22] and [across your devices](#)^[23]. The information we use for these purposes is automatically processed by our systems. But in some cases, we also use [manual review](#)^[24] to access and review your information.

To use less information that's connected to individual users, in some cases we de-identify or aggregate information. We might also anonymize it so that it no longer identifies you. We use this information in the same ways we use your information as described in this section.

Here are the ways we use your information:

To provide, personalize and improve our Products

We use information we have, including any [information with special protections](#) you choose to share, to provide and improve our Products. This includes personalizing features, content and [recommendations](#), such as your [Facebook Feed](#)^[25], [Instagram feed](#), Stories and ads. We don't use profile fields about religious views, political views or who you're "interested in" to show you ads.

Read more about how we use information to provide, personalize and improve our Products:

How we show ads and other sponsored or commercial content

When you use our Products, you see ads and sponsored or commercial content, like product listings in Shops. You also see ads shown through [Meta Audience Network](#) when you visit other apps. We want everything you see to be interesting and useful to you.

To decide what to show you and others, we use information we have about you, including:

- Your profile information
- Your activity on and off our Products, including information we receive through cookies and similar technologies, according to your settings
- Things we infer about you, like topics we think you may be interested in
- Information about your friends, followers or other connections, including their activity or interests

[See some examples.](#)^[26]

[Learn more](#) about some of the ways we show you ads that we think may be interesting to you, including using machine learning.

Take control in Privacy Center



Learn more about how ads work



How we use information to improve our Products

We're always trying to make our Products better and create new ones with the features you want. Information we collect from you helps us learn how.

We use information we collect to:

- See if a product is working correctly
- Troubleshoot and fix it when it's not
- Test out new products and features to see if they work
- Get feedback on our ideas for products or features

- Conduct surveys and other research about what you like about our Products and brands and what we can do better

How we use location-related information

We use location-related information that you allow us to receive if you turn on the Location Services device setting. This includes things like your GPS location and, depending on the operating system you're using, other [device signals](#)^[27].

We also receive and use [some location-related information](#) even if Location Services is turned off. This includes:

- [IP addresses](#)^[28], which we use to estimate your general location. We can use IP addresses to estimate your specific location if it's necessary to protect the safety and security of you or others.
- Your and others' activity on our Products, like check-ins and events
- Information you give us directly, like if you enter your current city on your profile, or provide your address in Marketplace

We use location-related information, such as your current location, where you live, the places you like to go and the businesses and people you're near, to do the things described in the “How do we use your information?” section of the Policy, like:

- Provide, personalize and improve our Products, including ads, for you and others. [See an example](#)^[29].
- Detect suspicious activity and help keep your account secure. [Learn how.](#)^[30]

More resources

How to manage Facebook location settings
Facebook Help Center



How to turn Instagram location services on or off
Instagram Help Center



To promote safety, security and integrity

We use information we collect to help protect people from harm and provide safe, secure Products.

[Learn more](#) >

To provide measurement, analytics and business services

Lots of people rely on our Products to run or promote their businesses. We help them measure how well their ads and other content are working.

[Learn more >](#)

To communicate with you

We communicate with you using information you've given us, like contact information you've entered on your profile.

[Learn more >](#)

To research and innovate for social good

We use information we have, information from researchers and datasets from publicly available sources, professional groups and non-profit groups to conduct and support research.

[Learn more >](#)

Promoting safety, security and integrity

Here are some ways we promote safety, security and integrity. We work to:

- Verify accounts and activity
- Find and address violations of our terms or policies. In some cases, the decisions we make about violations are reviewed by the [Oversight Board](#). They may use information we have when they review our decisions. [Learn more](#) about how the Oversight Board processes information.
- Investigate suspicious activity
- Detect, prevent and combat harmful or unlawful behavior
- [Identify and combat disparities and racial bias](#) against historically marginalized communities
- Detect and prevent spam and other bad experiences
- [Detect when someone needs help](#) and provide support
- Detect and stop threats to our personnel and property
- Maintain the integrity of our Products

[Learn more](#) about how we work to keep Meta a safe place for everyone.

Take control



Account security



Providing measurement, analytics and business services

To provide measurement and analytics services, we use the [information we collect about you](#) across your accounts on our Products.

Our measurement and analytics services help our Partners understand things like:

- How many people see and interact with their content, including posts, videos, Facebook Pages, listings, Shops and ads (including those shown through apps using [Meta Audience Network](#))
- How people interact with their content, websites, apps and services
- What [types of people](#)^[31] interact with their content or use their services

More in the Privacy Policy

How do we share information with Partners, vendors, service providers and third parties?



Communicating with you

We communicate with you in a few different ways. For example:

- We send messages about the Products we know you use, using the email you register to your account
- Depending on your settings, we send marketing communications about Products you might like
- We ask you to participate in research based on things like how you use our Products
- We let you know about our policies and terms of service
- When you contact us with questions, we reply to your email
- We facilitate customer support communications with you when you've told us, either directly or through a third party, that you have questions or concerns about our Products

We also use information about how you interact with our messages, like if you open an email from us. This helps us understand the best way to reach you

and whether our communications are helpful.

Take control



Communication preferences



Researching and innovating for social good

We research and innovate to help people around the world. Our goals include:

- Contributing to social good and areas of public interest
- Advancing technology
- Improving safety, health and well-being

Here are some examples of our research:

- [We analyze information](#) about where groups of people go during crises. This helps relief organizations get aid to the right places.
- We work with independent researchers to better understand the impact social media might have on elections and democratic processes
- We've collaborated with academics and industry experts to help improve internet access and quality in rural areas
- We support research in areas like artificial intelligence and machine learning to do things like create [COVID-19 forecasting models](#)

[Learn more](#) about our research programs

More in the Privacy Policy

Why and how we process your information



22

Using information across our Products

We use [information across your accounts on our Products](#) to:

- Personalize ads for you and others. [Learn more.](#)
- Measure the performance of those ads. [Learn more.](#)

- Provide more personalized features, content and suggestions across our Products. [See examples](#)^[32].
- More accurately count people and understand how they use our Products
- Help keep you and others safe. [Learn more](#).

If you set up your [Accounts Center](#), we also use your information to offer [connected experiences](#) and improve your experiences across accounts. [See an example](#).^[33]

More resources

How to add or delete accounts in your Accounts Center
Facebook Help Center



23

Why we use information across devices

One reason we use your information across devices is to help us give you a more personalized experience. For example, we might show you an ad on your phone, and later you might use your laptop to click on the ad and buy the product. By combining that information across your devices, we can understand what ads are relevant to you and help businesses measure how well their ad performed.

24

Manual review

Examples of when we use manual review

- Our reviewers help us promote safety, security and integrity across our Products. For example, reviewers can look for and remove content that violates our terms and policies and keep content that doesn't break our terms and policies available. Their work supplements our [technology that detects violations](#).
- When our algorithms detect that [someone might need help](#), a reviewer can review their post and offer support if needed.
- We also use manual review to analyze content to train our algorithms to review content the same way a person would. This improves our automatic

processing, which in turn helps us improve our products.

Who reviews this information

Our reviewers work at Meta, for [Meta Companies](#) or for a trusted vendor. We require every reviewer who's allowed access to your information to meet privacy and security standards.

[Learn more](#) about how Facebook prioritizes content for manual review.

25

How we personalize your Facebook Feed

Your Facebook Feed is unique to you. We order (or “rank”) the content you can see in your Feed, and you can [learn more](#) about the different types of signals we use to rank it. We also suggest content that's relevant to you.

Many things influence the content you see in your Feed.

For example:

- If your friends, connections or people you may know interact with a Facebook Page, post or certain topic, we can suggest similar content to you. So if your friend Ahmad comments on a post about national parks, we can suggest the national parks post to you.
- If you and others interact with the same group, Facebook Page or post, we can suggest another group, Page or post that they interact with for you. So if you and Sharmila are in the same cat lovers group and Sharmila likes a Page that sells scarves, we might suggest the scarves Page to you.
- If you've recently engaged with a certain topic on Facebook, we might then suggest other posts that are related to that topic. So if you recently liked or commented on a post from a basketball Page, we could suggest other posts about basketball.
- You might see posts based on where you are and what people near you are interacting with on Facebook. So if you're near a sports stadium, we can suggest games or events occurring at the stadium. [Learn more](#) about how we use location-related information.

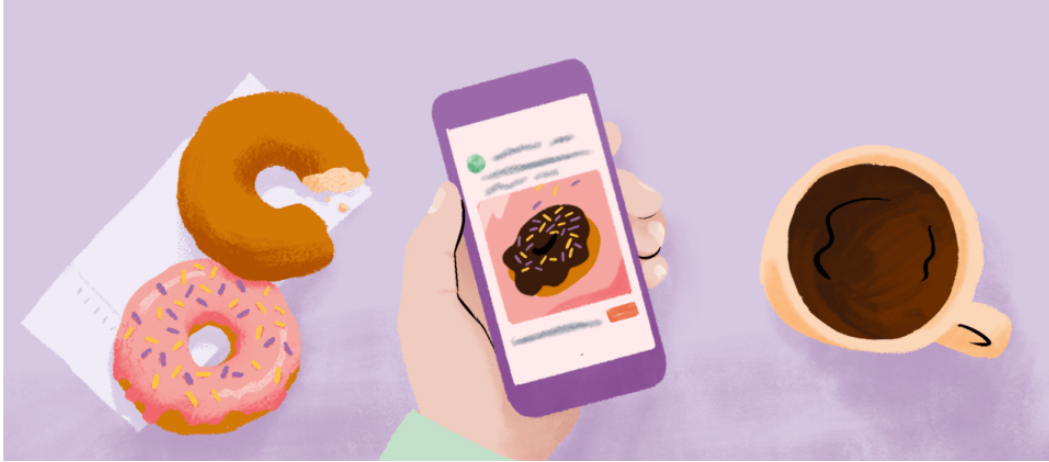
More resources

Manage your Facebook Feed preferences
[Facebook Help Center](#)



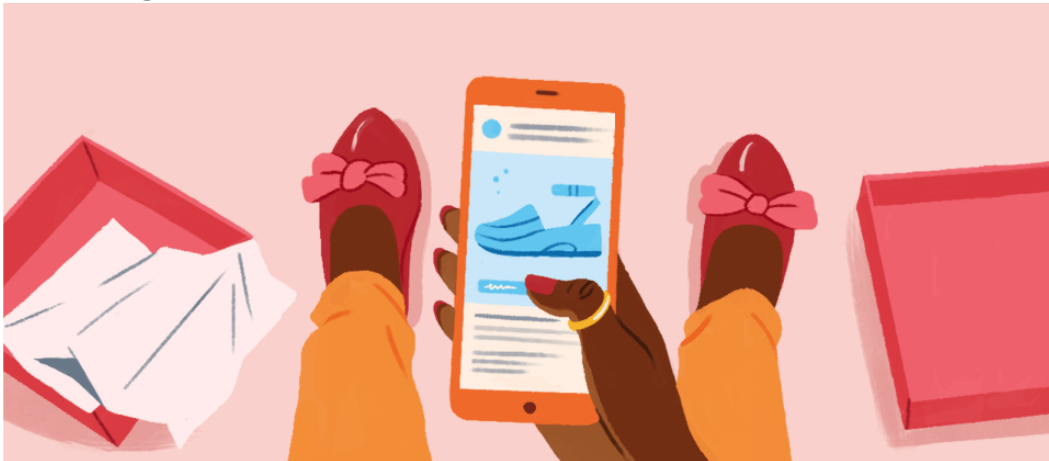
26

Your activity on our Products



For example, William checks into a local bakery on Facebook, so later we might show him ads on Instagram for other local bakeries.

Your activity on websites and apps, depending on your settings

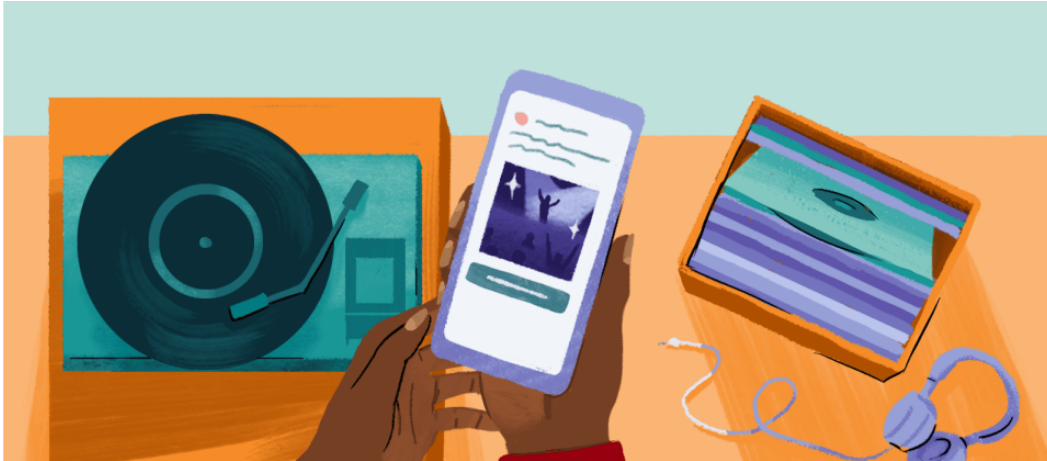


For example, Jane buys a pair of shoes from an online shoe store. The store shares Jane's activity with us using our Business Tools, subject to our Business Tools Terms.

Later, Jane sees an ad on Instagram for a discount on her next shoe purchase from the online store.

If she doesn't want to see more ads from this shoe store, she can hide them in her [advertisers setting](#). Or if she doesn't want us to show her any ads based on her activity on other websites and apps, she can make sure that this setting is turned off in her [ad settings](#)

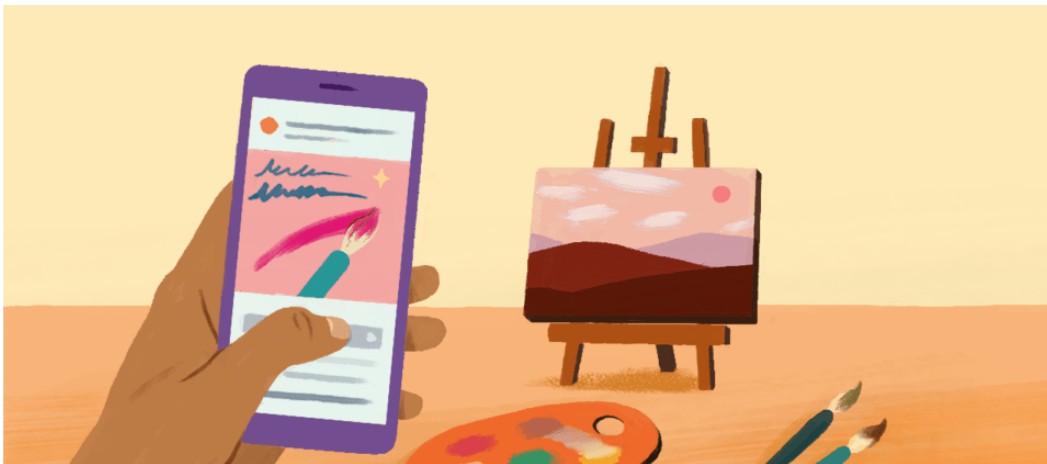
Topics we think you might be interested in



For example, Jon likes several Facebook Pages about famous musicians, so we think he has an interest in "music."

Based on this interest, we might show him an ad for a local record shop or an online music publication.

Your connections



For example, Fiona's friend likes an Instagram account for a local art fair. Based on her friend's activity, we might show Fiona an ad for the art fair.

Other device signals we receive

We receive different types of device signals from different operating systems. They include things like nearby Bluetooth or Wi-Fi connections.

28

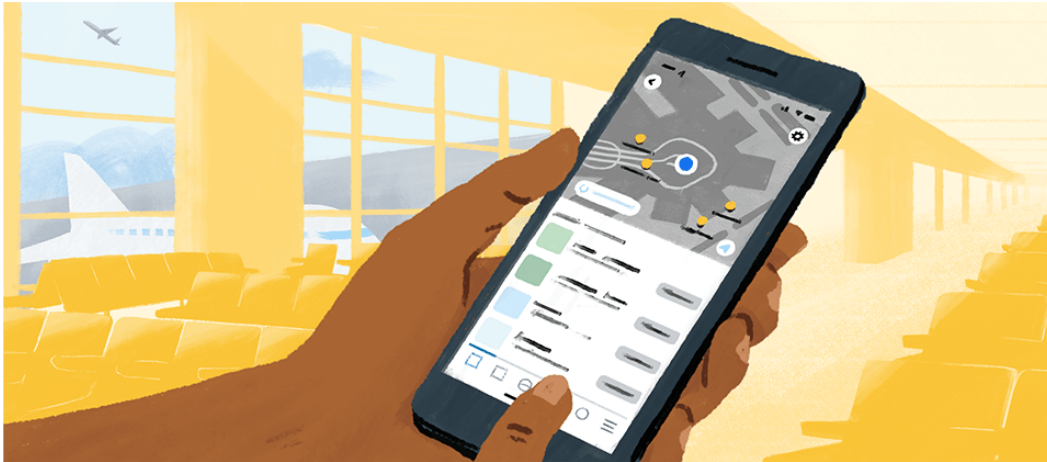
IP addresses

IP address stands for "internet protocol address." It's a unique number assigned to a device, like a phone or computer, that allows it to communicate over the internet. Numbers are assigned according to standard guidelines, or protocols.

Just like you need a mailing address to receive a letter from a friend, your device needs an IP address to receive information on the internet.

29

Personalizing ads for you and others



For example, Marcus is going on a trip and wants to use Find Wi-Fi to find free, public Wi-Fi at the airport. He has turned on Location Services, so we can use his GPS information to help him find the most relevant public Wi-Fi networks. We'll also use this information to show him ads for local businesses near the airport.

Later, Marcus turns off Location Services before he lands, so we don't collect his GPS information anymore. Later on his trip, he opens the Facebook app, and we can use the IP address we receive to estimate Marcus' current location and show him ads for businesses nearby.

30

Helping to keep your account secure

For example, we use information about the locations you normally log in from, combined with other information, to detect suspicious activity. So if we detect an attempt to log into your account from a new location, we can check that it's really you.

31

Information we provide about different types of people

For example, we might tell an advertiser that their ad was seen by women aged 25–34 who live in Madrid and like software engineering.

32

Providing more personalized features, content and suggestions across our Products

For example we can:

- Automatically fill in registration information, like your phone number, from one Meta Product when you sign up for an account on a different Product
- Let others see and search your name and profile photo across our Products and communicate with you
- Show all interactions in one place for content you've cross-posted to different Products

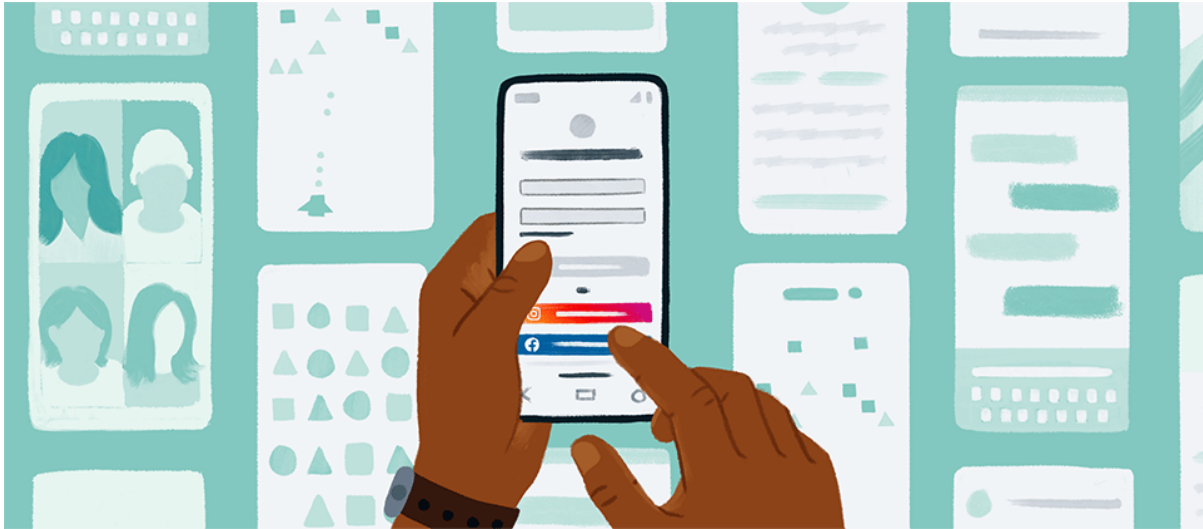
33

Using your information if you set up your Accounts Center

For example, if you follow your favorite team on Instagram, we can more easily suggest that you follow that team's Page on Facebook.

[Learn more](#) about how we use information across accounts if you set up Accounts Center.

How is your information shared on Meta Products or with Integrated Partners?



On Meta Products

Learn more about the different cases when your information can be shared on our Products:

People and accounts you share and communicate with

When you share and communicate using our Products, you can sometimes [choose the audience](#)^[34] for what you share.

When you interact with people or businesses, they can see:

What you share with them

For example, the audience you choose can see when you:

- Share a post you've written
- Share a photo or video
- Create a story
- Share a news article
- Add information to your profile

What you communicate with them

People you interact with can see what you send to them. So if you send a person or a business a message on Messenger or Instagram, that person or busi-

ness can read your message.

Some of your activity

People and businesses can also see some of your activity on our Products. This includes when you:

- Comment on or react to others' posts
- Engage with ads or other sponsored or commercial content, like by commenting or liking
- Allow content you've shared about a product in a Shop to be shared across our Products
- View their story on Facebook or Instagram
- Connect a new Meta device, like Portal or Ray-Ban Stories, to your account

When you're active

Some of our Products might provide you with settings that allow others to see when you're active on our Products, such as "active status." In some cases, we also offer settings that allow others to see when you're active in a particular section of one of our Products, like a message thread, game or event, or when you last used one of our Products.

Learn how to update your Active Status on [Facebook](#) and [Messenger](#), or how to update your Activity Status on [Instagram](#).

Content others share or reshare about you

Who can see or reshare your content

People in your audience can view your content and can choose to share it with others outside your audience, on and off our Products. For example, when you share a post or send a message to specific friends, they can download, screenshot or reshare it with anyone, on, across or off our Products.

When you comment on a post or react to a photo, your comment or reaction can be seen by anyone who can see the post or photo. This can include people you aren't connected to. The person who shared the post can also change their audience at any time after you've interacted with it.

How information about you can be shared

People who use our Products can share information about you with the audience they choose. For example, they can:

- Share a photo or video of you in a post, comment, story, reel or message
- Mention you in a post or story

- Tag you in a post, comment, story or location
- Share details about you in a post, story or message

If you're uncomfortable with what others have shared about you on our Products, you can always choose to [report posts and stories](#).

More resources

Remove a tag from a photo or post on Facebook
Facebook Help Center



Remove a tag from a photo or video on Instagram
Instagram Help Center



Public content

What content is public?

Some of your information and activity are always public. This includes your name, Facebook and Instagram username, profile picture and activity on public Facebook Pages and groups.

Other content you can choose to set to Public, like posts, photos and videos you post to your profile, Stories or Reels.

Who can see public content?

When content is public, it can be seen by anyone on or across our Products, and in some cases off our Products, even if they don't have an account.

For example, if you comment on Marketplace, a public Facebook Page or a public Instagram account, or if you leave a rating or review, your comment, rating or review will be visible to anyone. It could appear in any of our Products or be seen by anyone, including off our Products.

Where can public content be shared?

We, you and people using our Products can send public content (like your profile photo, or information you share on a Facebook Page or public Instagram account) to anyone on, across or off our Products. For example, users can share it in a public forum, or it can appear in search results on the internet.

Public content can also be seen, accessed, reshared or downloaded through third-party services, like:

- Search engines. [Learn more](#)^[35].
- APIs
- The media, like TV

- Other apps and websites connected to our Products

More resources

Public information on Facebook
Facebook Help Center



How to make a public account private on Instagram
Instagram Help Center



With Integrated Partners

You can choose to connect with [Integrated Partners](#)^[36] who use our Products. If you do, these Integrated Partners receive information about you and your activity.

These Integrated Partners can always access information that's public on our Products. Learn more about other information they receive and how they handle your information:

When you use an Integrated Partner's product or service

Information they receive automatically

When you use an Integrated Partner's products or services, they can access:

- What you post or share from these products or services
- What you use their services to do
- Information from and about the device you're using

[See examples](#)^[37] of when an Integrated Partner might receive your information.

Information they receive with your permission

Sometimes these Integrated Partners ask you for permission to access certain additional information from your Facebook, Instagram or Messenger account. In their request, they'll explain what information they'd like to access and let you choose whether to share it.

On Facebook, this includes things like your email address, hometown or birthday. On Instagram, this includes content, like photos and videos, that you've shared from your account when the account was set to private.

[Learn what happens if you choose to share your friends list, or if your friends choose to share their friends list.](#)^[38]

We automatically log when you receive a request from an Integrated Partner to access your information. These requests to access information are separate from the Apps and Websites access that you manage in your Facebook or Instagram ad settings or in your mobile device settings.

How long they can access your information

Apps or websites you've logged into using Facebook Login or connected to your Instagram account can access your nonpublic information on Meta Products unless it appears to us that you haven't used the app or website in 90 days. Note that even if an app's access to your data has expired, it can still retain information you shared with it previously.

We encourage you to visit your [Apps and Websites settings](#) from time to time to review which apps and websites continue to have access to your information through Facebook Login or Instagram.

More resources

How to manage apps and websites on Facebook
Facebook Help Center



How to manage apps and websites on Instagram
Instagram Help Center



When you interact with someone else's content on an Integrated Partner's product or service

Integrated Partners receive information about your activity when you interact with other Facebook, Instagram or Messenger users while they're using the Integrated Partner's product or service.

For example, a gamer livestreams to Facebook using a partner app. Then you comment on that livestream. The app developer will receive information about your comment.

How Integrated Partners handle your information

Integrated Partners handle the information you share with them according to their own terms and policies, not Meta's. You can review their privacy policy on their website or app to learn how they receive and process your information. In some cases, they use a separate service provider to receive and process your information.

More resources

How Meta reviews apps that integrate with our Products
Facebook Developers



Take control



Learn more about audiences in Privacy Center



Manage apps and websites



34

Choosing an audience

On Facebook, the audience can be made up of:

- The public, including people on and off Facebook
- Your friends and other connections, such as the friends of people you tag
- A customized list of people
- Yourself
- The members of a single community, such as a group

On Instagram, you can set the audience for what you share by choosing between a private or public account. With a [private account](#), only followers you approve can see what you share. With a public account, your posts and other content on Instagram can be seen by anyone, on or off our Products, including if they don't have an account. You can restrict the audience for your content by blocking individual accounts from viewing them. You can also create a close friends list for certain types of content that only the people on that list can see.

Take control

Audience settings

Manage your audience settings on Facebook or Instagram.



Audience settings are different from app permissions

Your audience settings are different from the permissions you give to individual apps and websites to access your information. [Read our policy](#) about how you may share information with Integrated Partners.

35

Search engines

You can visit your [privacy settings](#) to control whether search engines outside Facebook can link to your profile. But other public content—like if you post with your audience set to Public, or post on public Pages or accounts—might still be accessible through search engines, depending on the settings of that account.

36

Our Partners

Businesses and people can use our Products to advertise, market or support their products and services. When they use our Products, we call them our Partners.

Our Products include our Business Tools and other technologies that allow businesses to advertise or support their products and services, or to understand and measure how people are using their services and how well their ads are working. For example, they might put one of our Business Tools, the Meta Pixel, on their website. Or they might use Meta Audience Network tools to monetize their apps by showing ads from businesses that advertise on Facebook.

Our Products also include technologies where you can make a connection to our Partners through our Products. For example, you might log into their app or website using Facebook Login. Or you might play their game on Facebook, which we call an integration because you can play without leaving our app. We call the Partners who use these integrated tools our Integrated Partners.

Here are some examples of our Partners:

- Advertisers
- Companies that measure how well ads are doing and provide reports
- Businesses and people that use our Products to sell or offer goods and services
- Publishers (like a website or app) and their business partners
- App developers
- Game developers

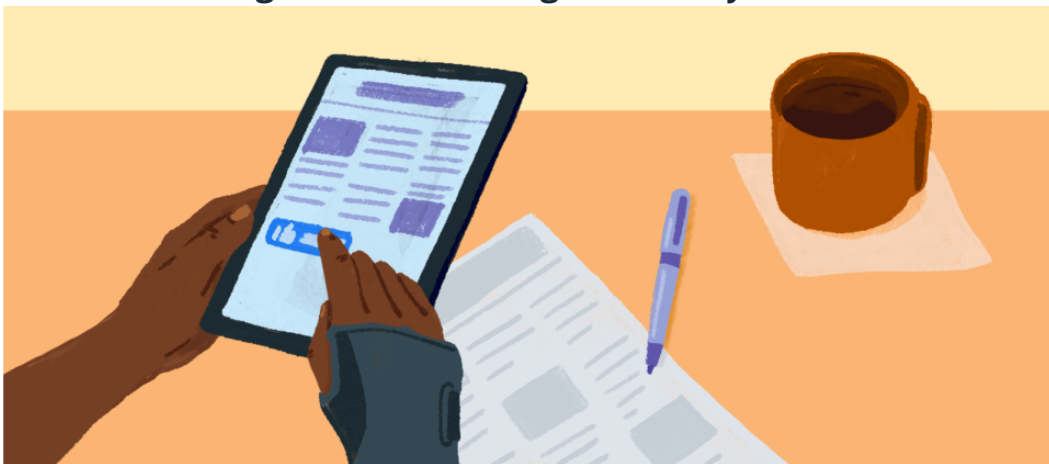
37

When an Integrated Partner might receive your information



For example, you might use your Facebook login to play an online game with your Facebook friends. The game developer automatically receives information about your activities in the game.

When an Integrated Partner might receive your information



Or you might use the Facebook Like button on an article posted on a news website. The website developer automatically receives information about your Like on their article.

38

Sharing friends lists

When you share your friends list

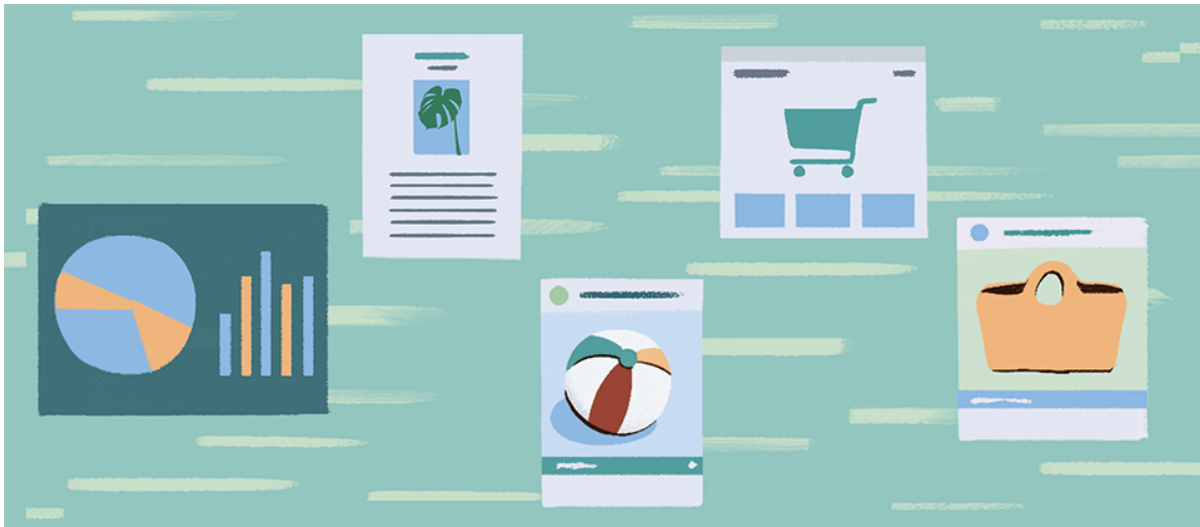
If you use Facebook Login to log into an app, the app developer might request access to your list of Facebook friends. Here's what happens if you give the app developer permission to view these lists:

- They can view and access a list of your Facebook friends who use the same app and have given the app permission to access their list of friends. They can't access nonpublic information about your friends or followers through this process. Note that the app developer will receive more information about your friends if your friends choose to share it themselves. They can share it by providing the information directly or giving the developer permission to access information from their account.
- You'll appear on friends lists that your Facebook friends can choose to share with the same app. You can remove this permission, or the app entirely, if you later decide that you don't want to share your friends list with an app, or don't want to appear on other friends lists shared with that app.

When your friends share their friends list

Your friends might choose to share their friends lists with app developers through Facebook Login. But your friends can't use Facebook Login to share nonpublic information about you.

How do we share information with Partners, vendors, service providers and third parties?



We don't sell any of your information to anyone, and we never will. We also require Partners and third parties to follow rules about how they can and cannot use and disclose the information we provide.

Here's more detail about who we share information with:

Partners

Advertisers and Audience Network publishers

Advertisers

We provide advertisers with reports about the number and kinds of people who see and engage with their ads. These reports include information about the general demographics and interests of people who engaged with an advertiser's ad. Then advertisers can better understand their audience. [See an example^{\[39\]}](#).

Meta also provides advertisers and their business partners with information about:

- Ads people engaged with, if any
- When people engaged with ads
- Where that ad was shown (for example, on Instagram, or on Facebook)

But we don't share information with these advertisers and their business partners that by itself can be used to contact or identify you, such as your name or email address, unless you [give us permission^{\[40\]}](#).

Audience Network publishers and their business partners

Meta Audience Network lets advertisers place ads with us that will be published on apps outside of Meta.

To help show you ads on their apps, we share information with publishers who use Audience Network, as well as business partners who facilitate that use. For example, we share:

- How many people see and engage with ads on publisher apps
- Information related to or in response to a [publisher's request](#) to serve an ad on its app.

But we don't share information with these publishers and their business partners that by itself can be used to contact or identify you, such as your name or email address, unless you [give us permission^{\[40\]}](#).

Partners who use our analytics services

People rely on our Products, like business accounts, professional tools and Facebook Pages, to run and promote their businesses. Businesses use our analytics services to understand more about how people are using their content and features.

We receive information about how people interact with their posts, listings, Facebook Pages, videos, Shops or other content, on and off our Products. Then we put this information into aggregate reports so they can see how well their content is performing.

These reports aggregate information like:

- How many people interacted with their content
- [The general demographics and interests^{\[39\]}](#) of the people who interacted with it

Partners who advertise with us also receive other information. [Read our policy](#) about how we share information with advertisers.

Partners who offer goods or services on our Products and commerce services platforms

When you choose to [make a transaction^{\[41\]}](#), or otherwise choose to share information with a seller, creator, fundraiser, charity, payment services provider or [commerce services platform^{\[42\]}](#), we share information with them and with any providers acting on their behalf.

Depending on how you interact with them, they receive:

- Information to complete your transaction, like order, payment, contact and shipping information
- Information to help ensure the security of the transaction, like information about your device or connection
- Any information required by applicable regulation
- Other information you choose to share with them

For example, if you make a purchase from an Instagram shop using checkout, the shop will receive information to complete your transaction. This may include your order items, your contact details and shipping information. If the shop uses a payment services provider, such as PayPal, to facilitate the transaction, the provider will receive the transaction amount, a transaction description (to appear on your credit card statement) and your payment card information, such as cardholder name, card number, expiration date and billing address. [Learn more](#) about payments on Instagram.

Integrated Partners

When you choose to use Integrated Partners' products or services, they receive information about you and your activity. [Read the policy.](#)

Vendors

Measurement and marketing vendors

Measurement and marketing vendors are businesses that provide marketing-related support to Meta and its advertisers. For example, they purchase ads on our behalf, provide market research and measure the effectiveness of our campaigns. Such vendors also support our Partners' advertising.

Measurement vendors

We don't create every measurement and analytics report ourselves.

We work with measurement vendors who create reports that help our Partners, like advertisers, understand how their content and ads are performing, who is engaging with them and whether people took an action after seeing their ad.

We share information (like whether people saw an ad or engaged with it) with our measurement vendors, who aggregate it to provide their reports. [See an example^{\[43\]}](#).

Marketing vendors

We share information about you with companies that help market our Company and Products, measure the effectiveness of our own marketing campaigns and perform advertising research. For example, we share your device identifier or other identifiers with advertising vendors to help us serve you ads most relevant to your interests. [Learn more^{\[44\]}](#) about how vendors support our marketing and advertising efforts.

Service providers

Service providers

Service providers provide services to us that help us provide our Products to you. We share the information we have about you to receive these services, which include:

- Investigating suspicious activity
- Detecting and stopping threats to our personnel and property
- Facilitating payments
- Providing customer support

- Improving the functionality of our Products
- Providing technical infrastructure services
- Analyzing how our Products are used
- Conducting research and surveys
- Marketing and promoting our Products
- Analyzing the effectiveness of our ads

Third parties

External researchers

We provide information to external researchers. They use it to conduct research that advances scholarship and innovation, and to promote safety, security and integrity.

Research goals include supporting:

- Our business or mission
- Social good. [Learn more.](#)
- Technological advancement
- Safety and security on our Products
- Public interest
- Health and well-being

When sharing data with external researchers, we ensure the privacy of our users is protected. [Learn more](#) about the privacy-safe research we support.

Other times we share with third parties

We also share information with third parties in response to legal requests, to comply with applicable law or to prevent harm. [Read the policy.](#)

And if we sell or transfer all or part of our business to someone else, then we may give the new owner your information as part of that transaction, in line with applicable law.

General demographics and interests

For example, a bike shop creates a Page on Facebook and wants to place an ad to reach an audience of people in Atlanta interested in cycling. We determine whether someone fits in this audience based on, for example, whether they liked a Page about bikes. Then people in that audience could see the bike shop's ad.

You can see the “interests” assigned to you in your [ad preferences](#) and remove them if you want.

The bike shop can then see reports showing aggregated statistics about the audience seeing their ads and how their ads are performing. The reports would show statistics to the advertiser that, for example, most of the people who saw or clicked on their ad:

- Were women
- Were between the ages of 25 and 34
- Clicked on the ad from their phone

40

When you might give us permission

For example, you might request more information from a business by clicking their ad in your Facebook Feed and submitting a form with your name and contact information. Then the advertiser would receive the information you provided.

41

Transactions you might make

- Subscribing to premium content
- Buying, selling or using products
- Buying, selling or using services
- Donating to charities

42

Commerce services platforms

Commerce services platforms provide a range of commerce services, including:

- Payments
- Marketing
- Shipping
- Customer engagement tools

43

How measurement vendors use information to make reports

For example, an advertiser might ask a measurement vendor to help figure out the impact its ads on Facebook have had on sales. The measurement vendor compares information from us about clicks on the advertiser's Facebook ads with information from the advertiser about product purchases. Then the measurement vendor creates and provides aggregated reports that show the advertiser how its ads are performing.

44

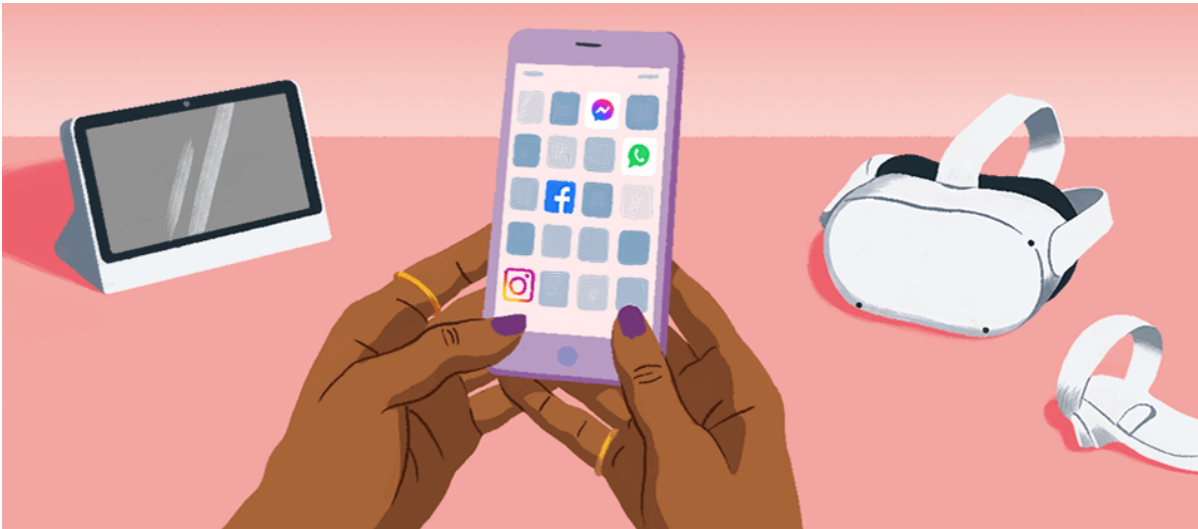
How vendors support our marketing and advertising efforts

For example, vendors:

- Serve our advertisements across the Internet, including on mobile, desktop and connected television devices
- Track and categorize your online and mobile app activity
- Provide us information about your interests and community and advertising interactions

These vendors help us understand who might find our advertising most relevant to their interests, and which of our Products might interest you. This information can be used to personalize which of our ads are shown to you. Vendors also use this information to measure response to our marketing efforts and the effectiveness of our advertising.

How do the Meta Companies work together?



We are part of the [Meta Companies](#) that provide Meta Company Products. [Meta Company Products](#) include all the Meta Products covered by this Policy, plus other products like WhatsApp, Novi and more.

We share information we collect, infrastructure, systems and technology with the other Meta Companies. [Learn more](#) about how we transfer information to other countries.

We also process information that we receive about you from other Meta Companies, according to their terms and policies and as permitted by applicable law. In some cases, Meta acts as a service provider for other Meta Companies. We act on their behalf and in accordance with their instructions and terms.

Why we share across the Meta Companies

Meta Products share information with other Meta Companies:

- To promote safety, security and integrity and comply with applicable laws
- To personalize offers, ads and other sponsored or commercial content
- To develop and provide features and integrations
- To understand how people use and interact with Meta Company Products

[See some examples^{\[45\]}](#) of why we share.

More resources

Review the privacy policies of the other [Meta Companies](#)



45

Why we share across the Meta Companies

Promoting safety, security and integrity and complying with applicable law

For example, we share information with Meta Companies that provide financial products and services to help them promote safety, security and integrity and comply with applicable law. This includes:

- Complying with their legal obligations
- Helping keep you and others safe
- Performing account verification
- Investigating suspicious activities
- Creating analytics

For these purposes, we might share your name, email address, who you're friends with and other account information within the Meta Companies.

Developing and providing features and integrations

For example, where available in your country, you can choose to use certain integrations that connect your WhatsApp experiences with other Meta Company Products. These integrations let you do things like:

- Use your Facebook Pay account to pay for things on WhatsApp
- Chat with your friends on other Meta Company Products, such as Portal, by connecting your WhatsApp account

We also share information with Meta Companies to support innovation. For example, your videos can help train our products to recognize objects, like trees, or activities, like when a dog chases a ball. This technology is used to help us offer new products or features in the future.

Understanding how people use our products

We count the number of unique users, monthly active users and daily active users on our products. This information helps us understand the community using our products and publicly share important trends about how our products are used.

How can you manage or delete your information and exercise your rights?

We offer you a variety of tools to view, manage, download and delete your information below. You can also manage your information by visiting the settings of the Products you use. You may also have other privacy rights under applicable laws.

To exercise your rights, visit our Help Centers, your settings for Facebook and Instagram and your device-based settings.

Take a privacy checkup



Take a privacy checkup
Be guided through Facebook privacy settings



View and manage your information



Access your information



Off-Facebook activity



Ad preferences



Manage your data



Port, download or delete your information



Port your information ^[46]



Download your information



Delete your information or account ^[47]



You can learn more about how privacy works on [Facebook](#) and on [Instagram](#), and in the [Facebook Help Center](#). If you have questions about this policy, you can [contact us](#) as described below. In some countries, you may also be able to contact the Data Protection Officer for Meta Platforms, Inc., and depending on your jurisdiction, you may also contact your local Data Protection Authority (“DPA”) directly.

Port your information

In certain cases and subject to applicable law, you have the right to [port your information](#).

47

Delete your information or account

To delete your information, you can:

- **Find and delete specific information.** We offer tools you can use to delete certain information. For example, you can use Delete buttons to delete content you've posted to your account. You can also use tools like [activity log](#) on Facebook to send content to the trash in bulk. When you delete content, it's no longer visible to other users. Visit the [Facebook Help Center](#) or [Instagram Help Center](#) to learn what happens when you delete your content or move it to trash.
- **Permanently delete your account.** If you delete your account on [Facebook](#) or [Instagram](#), we delete your information, including the things you've posted, such as your photos and status updates, unless we need to keep it as described in "[How long do we keep your information?](#)" Once your account is [permanently deleted](#) you won't be able to reactivate it, and you won't be able to retrieve information, including content you've posted.

How long does it take to delete your information?

If you request that we delete your account or content, it may take up to 90 days to delete your information after we begin the account deletion process or receive a content deletion request. After the information is deleted, it may take us up to another 90 days to remove it from backups and disaster recovery.

If you leave your deleted content in your trash on Facebook or your Recently Deleted folder on Instagram, the deletion process will begin automatically in 30 days. Or you can start the deletion process right away by deleting the content from your trash or Recently Deleted folder.

How long do we keep your information?

We keep 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. For example, we need to keep some of your information to maintain your account. [Learn more](#)^[48].
- The feature we use it for, and how that feature works. For example, messages sent using Messenger's vanish mode are retained for less time than regular messages. [Learn more](#)^[49].
- How long we need to retain the information to comply with certain legal obligations. [See some examples](#)^[50].
- 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

In some instances and for specific reasons, we'll keep information for an extended period of time. [Read our policy](#)^[51] about when we may preserve your information.

48

If we need it to operate or provide our Products

For example, we keep profile information, photos you've posted (and not deleted) and security information for the lifetime of your account.

And when you search for something on Facebook, we keep your search history until you clear the search in your [activity log](#) or delete your account. Once you clear a search or delete your account, it will no longer be visible to you, and it will be [deleted](#)^[52].

But even if you don't clear your search or delete your account, within six months of your search we delete information about that search that isn't necessary to show you your search history, like information about the device you were using, or your location.

49

The feature we use it for, and how that feature works



For example, May is planning a surprise party for Yang. She sends Cynthia the party details in Messenger using vanish mode so that the message will disappear. The message will no longer be visible to May once she leaves the chat, and Cynthia will see the message only the first time she opens the chat thread.

After Cynthia reads the message, the content is deleted after one hour. If Cynthia never reads it, it's deleted after 14 days.

50

How long we need to retain the information to comply with certain legal obligations

For example, we retain information for as long as we need it for:

- A legal request or obligation, including obligations of Meta Companies or to comply with applicable law
- A governmental investigation
- A legal claim, complaint, litigation or regulatory proceedings

51

Why we may preserve your information longer

Your information, including financial transaction data related to purchases or money transfers made on our Products, may be preserved and accessed for a longer time period if it's related to any of the following:

- A legal request or obligation, including obligations of Meta Companies or to comply with applicable law
- A governmental investigation
- An investigation of possible violations of our terms or policies
- To prevent harm
- For safety, security and integrity purposes
- To protect ourselves, including our rights, property or products
- If it's needed in relation to a legal claim, complaint, litigation or regulatory proceedings

See some examples^[53].

In some cases, we may preserve your information based on the above reasons even after you request deletion of your account or some of your content. We may also preserve information from accounts that have been disabled and content that has been removed for violations of our terms and policies.

52

Delete your information or account

To delete your information, you can:

- **Find and delete specific information.** We offer tools you can use to delete certain information. For example, you can use Delete buttons to delete content you've posted to your account. You can also use tools like [activity log](#) on Facebook to send content to the trash in bulk. When you delete content, it's no longer visible to other users. Visit the [Facebook Help Center](#) or [Instagram Help Center](#) to learn what happens when you delete your content or move it to [trash](#).
- **Permanently delete your account.** If you delete your account on [Facebook](#) or [Instagram](#), we delete your information, including the things you've posted, such as your photos and status updates, unless we need to keep it as described in "[How long do we keep your information?](#)" Once your account is [permanently deleted](#) you won't be able to reactivate it, and you won't be able to retrieve information, including content you've posted.

How long does it take to delete your information?

If you request that we delete your account or content, it may take up to 90 days to delete your information after we begin the account deletion process or re-

ceive a content deletion request. After the information is deleted, it may take us up to another 90 days to remove it from backups and disaster recovery.

If you leave your deleted content in your trash on Facebook or your Recently Deleted folder on Instagram, the deletion process will begin automatically in 30 days. Or you can start the deletion process right away by deleting the content from your trash or Recently Deleted folder.

53

Examples of why we might preserve your information

To respond to a legal request

For example, we might preserve your information after you delete your account when we receive a valid legal request, such as a preservation order or search warrant, related to your account.

To comply with applicable law

For example, we preserve certain information about purchases or transactions associated with an account, in line with Meta's accounting obligations.

For safety, security and integrity purposes

For example, if we disable an account for violating our terms or policies, we preserve information about that user to prevent them from opening a new account.

We also might preserve some of your account information as part of our review of suspicious activity. This includes any suspicious activity associated with our financial products, like suspected money laundering or terrorist funding.

For litigation

We may preserve your information where we deem it necessary for reasons related to a legal claim or complaint. For example, we may be required to defend ourselves in legal proceedings in a claim related to your information.

How do we transfer information?

Why is information transferred to other countries?

We share the [information we collect](#) globally, both internally across our offices and data centers, and externally with our Partners, vendors, service providers

and third parties. Because Meta is global, with users, Partners and employees around the world, transfers are necessary for a variety of reasons, including:

- So we can operate and provide the services stated in the terms of the Meta Product you're using and this Policy. This includes allowing you to share information and connect with your family and friends around the globe.
- So we can fix, analyze and improve our Products

Where is information transferred?

Your information will be transferred or transmitted to, or stored and processed in:

- Places we have infrastructure or data centers, including the United States, Ireland, Denmark and Sweden, among others
- Countries where Meta Company Products are available
- Other countries where our Partners, vendors, service providers and third parties are located outside of the country where you live, for purposes as described in this Policy

How do we safeguard your information?

We rely on [appropriate mechanisms](#)^[54] for international data transfers.

We also make sure that appropriate safeguards are in place whenever we transfer your information. For example, we encrypt your information when it's in transit over public networks to protect it from unauthorized access.

More resources

How information is safeguarded as it's transferred
Facebook Newsroom



54

Mechanisms we use for global data transfers

We rely on appropriate mechanisms for international data transfers. For example, for [information we collect](#):

- We utilize [standard contractual clauses](#) approved by the European Commission and by other relevant authorities.
- We rely on determinations from the European Commission, and from other relevant authorities, about whether other countries have [adequate levels of data protection](#).
- We use equivalent mechanisms under applicable laws that apply to data transfers to the United States and other relevant countries.

How do we respond to legal requests, comply with applicable law and prevent harm?

We access, preserve, use and share your information:

- In response to legal requests, like search warrants, court orders, production orders or subpoenas. These requests come from third parties such as civil litigants, law enforcement and other government authorities. [Learn more^{\[55\]}](#) about when we respond to legal requests.
- In accordance with applicable law
- To promote the safety, security and integrity of Meta Products, users, employees, property and the public. [Learn more^{\[56\]}](#).

We may access or preserve your information for an extended amount of time. [Learn more^{\[57\]}](#).

55

When we respond to legal requests

We respond to legal requests where we have a good faith belief that we're required by law to do so.

We also respond to certain legal requests where not compelled by law, but where we have a good faith belief that a response:

- Is required by law in that jurisdiction,
- Affects users in that jurisdiction, and
- Is consistent with internationally recognized standards including, for example, our [Corporate Human Rights Policy](#).

Learn more about [government requests](#) and [how we've responded](#).

56

How we promote safety, security and integrity

We share your information with law enforcement, government authorities, Meta Companies, third parties (including industry peers) and others when we have a good faith belief it's necessary to detect, prevent and address a variety of situations, such as:

- Unauthorized use of our Products. [See an example.](#)^[58]
- Violations of our terms and policies. [See an example.](#)^[59]
- Investigating suspicious activity
- Protecting ourselves, including our rights, property, personnel or Products
- Preventing abuse, fraud, or other harmful or illegal activity, on and off our Products
- Protecting you or others, including as part of investigations or regulatory inquiries
- Emergency situations, such as risk of death or imminent bodily harm

57

Why we may preserve your information longer

Your information, including financial transaction data related to purchases or money transfers made on our Products, may be preserved and accessed for a longer time period if it's related to any of the following:

- A legal request or obligation, including obligations of Meta Companies or to comply with applicable law
- A governmental investigation
- An investigation of possible violations of our terms or policies
- To prevent harm
- For safety, security and integrity purposes
- To protect ourselves, including our rights, property or products

- If it's needed in relation to a legal claim, complaint, litigation or regulatory proceedings

See some examples^[60].

In some cases, we may preserve your information based on the above reasons even after you request deletion of your account or some of your content. We may also preserve information from accounts that have been disabled and content that has been removed for violations of our terms and policies.

58

Unauthorized use of our Products

For example, if you unlawfully collect and use Facebook user data, we may share your information to defend ourselves against claims or in litigation.

59

Violations of our terms and policies

For example, if you post threatening or harmful content, we may share your information across the Meta Companies to protect ourselves and others. This can include blocking your access to certain features or disabling your account across the Meta Companies.

60

Examples of why we might preserve your information

To respond to a legal request

For example, we might preserve your information after you delete your account when we receive a valid legal request, such as a preservation order or search warrant, related to your account.

To comply with applicable law

For example, we preserve certain information about purchases or transactions associated with an account, in line with Meta's accounting obligations.

For safety, security and integrity purposes

For example, if we disable an account for violating our terms or policies, we preserve information about that user to prevent them from opening a new account.

We also might preserve some of your account information as part of our review of suspicious activity. This includes any suspicious activity associated with our financial products, like suspected money laundering or terrorist funding.

For litigation

We may preserve your information where we deem it necessary for reasons related to a legal claim or complaint. For example, we may be required to defend ourselves in legal proceedings in a claim related to your information.

How will you know the policy has changed?

We'll notify you before we make material changes to this Policy. You'll have the opportunity to review the revised Policy before you choose to continue using our Products.

Privacy notice for California residents

If you are a California resident, you can learn more about your consumer privacy rights by reviewing the [California Privacy Notice](#).

How to contact Meta with questions

You can learn more about how privacy works on [Facebook](#) and on [Instagram](#) and in the [Facebook Help Center](#). If you have questions about this Policy or have questions, complaints or requests regarding your information, you can contact us as described below.

You can contact us [online](#) or by mail at:

Meta Platforms, Inc.
ATTN: Privacy Operations
1601 Willow Road
Menlo Park, CA 94025

Why and how we process your information

The categories of information we use, and why and how information is processed, are set out below:

--	--

<p>Why and how we process your information</p>	<p>Information categories we use (see 'What Information do we collect?' for more information on each information category) The actual information we use depends on your factual circumstances, but could include any of the following:</p>
<p>Personalizing the Meta Products: Our systems automatically process information we collect and store associated with you and others to assess and understand your interests and your preferences and provide you personalized experiences across the Meta Products in accordance with our terms. This is how we:</p> <ul style="list-style-type: none"> • Personalize features and content (such as your News Feed, Instagram Feed and Stories); • Personalize the ads people see; and • Make suggestions for you (such as people you may know, groups or events that you may be interested in or topics that you may want to follow) on and off our products. <p>Learn more about how we use information about you to personalize your experience on and across Meta Products and how we choose the ads that you see.</p>	<p>Your activity and information you provide:</p> <ul style="list-style-type: none"> • 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 • Metadata about content • Types of content you view or interact with, and how you interact with it • Apps and features you use, and what actions you take in them • Purchases or other transactions you make • Hashtags you use • The time, frequency and duration of your activities on our Products <p>Friends, followers and other connections</p> <p>App, browser and device information:</p> <ul style="list-style-type: none"> • Device characteristics and device software

	<ul style="list-style-type: none"> • What you're doing on your device (like whether our app is in the foreground or if your mouse is moving) • Identifiers that tell your device apart from other users' • Device signals • Information you've shared through your device settings (like GPS location) • Information about the network you connect your device to • Reports about our products' performance on your device • Information from cookies and similar technologies <p>Information from Partners, vendors and third parties. (You have control over Meta's use of Partner data to tailor ads to you.)</p>
<p>Providing and improving our Meta Products: The provision of the Meta Products includes collecting, storing, and, where relevant, sharing, profiling, reviewing and curating, and in some instances not only automated processing but also manual (human) reviewing, to:</p> <ul style="list-style-type: none"> • Create and maintain your account and profile, • Facilitate the sharing of content and status, • Provide and curate features, • Provide messaging services, the ability to make voice and video calls and connect with others, • Provide advertising products, and 	<p>Your activity and information you provide:</p> <ul style="list-style-type: none"> • 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 • Messages you send and receive, including their content, subject to applicable law • Metadata about content and messages, subject to applicable law • Types of content you view or interact with, and how you in-

<div><ul style="list-style-type: none">• Undertake analytics.<p>We also use information to develop, research and test improvements to our Products. We use information we have to:</p><ul style="list-style-type: none">• See if a product is working correctly,• Troubleshoot and fix it when it's not,• Test out new products and features to see if they work,• Get feedback on our ideas for products or features, and• Conduct surveys and other research about what you like about our Products and brands and what we can do better.</div>	<div><p>teract with it</p><ul style="list-style-type: none">• Apps and features you use, and what actions you take in them• Purchases or other transactions you make, including truncated credit card information• Hashtags you use• The time, frequency and duration of your activities on our Products<p>Friends, followers and other connections</p><p>App, browser and device information:</p><ul style="list-style-type: none">• Device characteristics and device software• What you're doing on your device (like whether our app is in the foreground or if your mouse is moving)• Identifiers that tell your device apart from other users'• Device signals• Information you've shared through your device settings• Information about the network you connect your device to, including your IP address• Information from cookies and similar technologies<p>Information from Partners, vendors and third parties</p></div>
<div>Promoting safety, integrity and security</div>	<div>Your activity and information you</div>

on and across the Meta Products: The Meta Products are designed to research and help ensure the safety, integrity and security of those services and those people who enjoy them, on and off Meta Products. We process information we have associated with you and apply automated processing techniques and, in some instances, conduct manual (human) review to:

- Verify accounts and activity,
- Find and address violations of our terms or policies. In some cases, the decisions we make about violations are reviewed by the [Oversight Board](#),
- Investigate suspicious activity,
- Detect, prevent and combat harmful or unlawful behavior, such as to review and, in some cases, remove content reported to us,
- Identify and combat disparities and racial bias against historically marginalized communities,
- Protect the life, physical or mental health, well-being or integrity of our users or others,
- Detect and prevent spam, other security matters and other bad experiences,
- Detect and stop threats to our personnel and property, and
- Maintain the integrity of our Products.

For more information on safety, integrity and security generally on Meta Products, visit the [Facebook Security Help Center](#) and [Instagram Security Tips](#).

provide::

- 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
- Messages you send and receive, including their content, subject to applicable law
- Metadata about content and messages, subject to applicable law
- Types of content you view or interact with, and how you interact with it
- Apps and features you use, and what actions you take in them
- Purchases or other transactions you make, including truncated credit card information
- Hashtags you use
- The time, frequency and duration of your activities on our Products

[Friends, followers and other connections](#)

[App, browser and device information:](#)

- Device characteristics and device software
- What you're doing on your device (like whether our app is in the foreground or if your mouse is moving)

	<ul style="list-style-type: none"> • Identifiers that tell your device apart from other users' • Device signals • Information you've shared through your device settings • Information about the network you connect your device to, including your IP address • Information from cookies and similar technologies <p>Information from Partners, vendors and third parties</p>
<p>To communicate with you: We use information you've given us (like contact information on your profile) to send you a communication, like an e-mail or in-product notice, for example:</p> <ul style="list-style-type: none"> • We'll contact you via email or in-product notifications in relation to the Meta Products, product-related issues, research or to let you know about our terms and policies. <p>We also use contact information like your email address to respond when you contact us.</p>	<p>Your activity and information you provide:</p> <ul style="list-style-type: none"> • Contact information on your profile and your communications with us • 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 <p>App, browser and device information:</p> <ul style="list-style-type: none"> • Device characteristics and device software • What you're doing on your device (like whether our app is in the foreground or if your mouse is moving) • Identifiers that tell your device apart from other users' • Device signals

	<ul style="list-style-type: none"> • Information you've shared through your device settings • Information about the network you connect your device to, including your IP address • Information from cookies and similar technologies.
<p>Transferring, storing or processing your information across borders, including from and to the United States and other countries: We share information we collect globally, both internally across our offices and data centers and externally with our Partners, third parties and service providers. Because Meta is global, with users, Partners, vendors and employees around the world, transfers are necessary:</p> <ul style="list-style-type: none"> • To operate and provide the services described in the terms that apply to the Meta Product(s) you are using. This includes allowing you to share information and connect with your family and friends around the globe; and • To fix, analyze and improve our Products. <p>For more information, see the "How do we transfer information?" section of the Meta Privacy Policy.</p>	<p>Your activity and information you provide:</p> <ul style="list-style-type: none"> • 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 • Metadata about content and messages, subject to applicable law • Types of content you view or interact with, and how you interact with it • Apps and features you use, and what actions you take in them • Purchases or other transactions you make, including truncated credit card information • Hashtags you use • The time, frequency and duration of your activities on our Products <p>Friends, followers and other connections</p> <p>App, browser and device information:</p>

	<ul style="list-style-type: none"> • Device characteristics and device software • What you're doing on your device (like whether our app is in the foreground or if your mouse is moving) • Identifiers that tell your advice apart from other users' • Device signals • Information you've shared through your device settings • Information about the network you connect your device to, including your IP address • Information from cookies and similar technologies <p>Information from Partners, vendors and third parties</p>
Processing information subject to special protections under applicable laws that you provide so we can share it with those you choose, to provide, personalize and improve our Products and to undertake analytics. We'll collect, store, publish and apply automated, or sometimes manual (human), processing for these purposes.	<p>Your activity and information you provide:</p> <ul style="list-style-type: none"> • Any information with special protections that you choose to provide in your profile fields (such as your religious views, political views, or who you are "interested in"), or as part of surveys you choose to participate in
Receiving and using information from third parties to tailor the ads you see: We'll use information that advertisers, businesses and other partners provide us about activity off Meta Products that we have associated with you to personalize ads that we show you on Meta Products, and on websites, apps and	<p>Your activity and information you provide:</p> <ul style="list-style-type: none"> • Information and content you provide, such as your name or email address <p>Information from Partners, vendors and third parties</p>

<p>devices that use our advertising services. We receive this information whether or not you're logged in or have an account on our Products. See the Cookies Policy for more information.</p>	
<p>Sharing your contact, profile or other information with third parties upon your request: The type of third party and categories of information shared depend on the circumstances of what you ask us to share. For example:</p> <ul style="list-style-type: none"> • We share your email (or other contact information) or other information you might choose when you direct us to share it with an advertiser so they can contact you with additional information about a promoted product, and • If you choose to integrate other apps, games or websites with Meta Products and log in, we'll share your information with the app, game or website to log you in. 	<p>Your activity and information you provide:</p> <ul style="list-style-type: none"> • Content you create, like your contact, profile or other information, like posts or comments
<p>Providing measurement, analytics and business services:</p> <p>Our systems automatically, as well as with some manual (human) processing, process information we have collected and stored about you and others. We use this information to:</p> <ul style="list-style-type: none"> • Provide insights and measurement reports to businesses, advertisers and other Partners to help them measure the effectiveness and distribution of their or their clients' ads, content and services, to understand the kinds of people who are seeing their content and ads, and how their con- 	<p>Your activity and information you provide:</p> <ul style="list-style-type: none"> • 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 • Types of content you view or interact with, and how you interact with it • Apps and features you use, and what actions you take in them

<p>tent and ads are performing on and off Meta Products, and</p> <ul style="list-style-type: none"> • Provide aggregated user analytics and insights reports that help businesses, advertisers and other Partners better understand the audiences with whom they may want to connect, as well as the types of people who use their services and how people interact with their websites, apps and services. 	<ul style="list-style-type: none"> • Purchases or other transactions you make • Hashtags you use • The time, frequency and duration of your activities on our Products <p>Friends, followers and other connections</p> <p>App, browser and device information:</p> <ul style="list-style-type: none"> • Device characteristics and device software • What you're doing on your device (like whether our app is in the foreground or if your mouse is moving) • Identifiers that tell your device apart from other users • Device signals • Information you've shared through your device settings • Information about the network you connect your device to, including your IP address • Information from cookies and similar technologies
<p>Sharing of information across the Meta Companies:</p> <ul style="list-style-type: none"> • To provide a seamless, consistent and richer, innovative experience across the Meta Company Products to enable cross app interactions, sharing, viewing and engaging with content, including posts and videos. 	<p>Your activity and information you provide:</p> <ul style="list-style-type: none"> • 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

	<ul style="list-style-type: none">• Metadata about content• Types of content you view or interact with, and how you interact with it• Apps and features you use, and what actions you take in them• Purchases or other transactions you make• Hashtags you use• The time, frequency and duration of your activities on our Products <p>Friends, followers and other connections</p> <p>App, browser and device information:</p> <ul style="list-style-type: none">• Device characteristics and device software• What you're doing on your device (like whether our app is in the foreground or if your mouse is moving)• Identifiers that tell your device apart from other users'• Device signals• Information you've shared through your device settings• Information about the network you connect your device to, including your IP address• Information from cookies and similar technologies
Business intelligence and analytics:	Your activity and information you

- To understand, in aggregate, your usage of and across our Products, to accurately count people and businesses; and
- To validate metrics directly related to these, in order to inform and improve product direction and development and to adhere to (shareholder/earning) reporting obligations.

provide:

- 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
- Metadata about content and messages, subject to applicable law
- Types of content you view or interact with, and how you interact with it
- Apps and features you use, and what actions you take in them
- Purchases or other transactions you make
- Hashtags you use
- The time, frequency and duration of your activities on our Products

Friends, followers and other connections

App, browser and device information:

- Device characteristics and device software
- What you're doing on your device (like whether our app is in the foreground or if your mouse is moving)
- Identifiers that tell your device apart from other users'
- Device signals

	<ul style="list-style-type: none"> • Information you've shared through your device settings • Information about the network you connect your device to, including your IP address • Information from cookies and similar technologies <p>Information from Partners, vendors and third parties</p>
<p>Identifying you as a Meta Product user and personalizing the ads we show you through Meta Audience Network when you visit other apps:</p> <ul style="list-style-type: none"> • When we show you ads through Meta Audience Network when you visit other apps, our systems automatically process the information we have collected and stored about you and others to identify you as a Meta Product user and tailor the ads you see. 	<p>Your activity and information you provide:</p> <ul style="list-style-type: none"> • Information you provide • 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 • Metadata about content • Types of content you view or interact with, and how you interact with it • Apps and features you use, and what actions you take in them • Purchases or other transactions you make • Hashtags you use • The time, frequency and duration of your activities on our Products <p>Friends, followers and other connections</p>

	<p>App, browser and device information:</p> <ul style="list-style-type: none"> • Device characteristics and device software • What you're doing on your device (like whether our app is in the foreground or if your mouse is moving) • Identifiers that tell your device apart from other users' • Device signals • Information you've shared through your device settings • Information about the network you connect your device to, including your IP address • Information from cookies and similar technologies
<p>Providing marketing communications to you:</p> <ul style="list-style-type: none"> • Depending on your settings and subject to applicable law, we'll share marketing communications with you. • We'll collect and store your information and use it to send marketing communications to you, like an email, subject to applicable laws. 	<p>Your activity and information you provide:</p> <ul style="list-style-type: none"> • Information and content you provide, including your contact information like email address <p>App, browser and device information:</p> <ul style="list-style-type: none"> • Device identifiers
<p>Research and innovate for social good:</p> <ul style="list-style-type: none"> • We carry out surveys and use information (including from researchers we collaborate with) to conduct and support research and innovation on topics of general social welfare, technological advancement, public interest, health and well-being. 	<p>Your activity and information you provide:</p> <ul style="list-style-type: none"> • Content you create, like posts, comments or audio • Content you provide through our camera feature or your

- For example, we analyze information that we have about migration patterns during crises. This helps relief organizations get aid to the right places.
- We collect, store, combine, analyze and apply automatic processing techniques like aggregation of information as well as manual (human) review, and share information, as necessary to research and innovate for social good in this way. We do this to do things like create COVID-19 forecasting models.

[Learn more](#) about our research programs.

camera roll settings, or through our voice-enabled features

- Metadata about content and messages, subject to applicable law
- Types of content you view or interact with, and how you interact with it
- Apps and features you use, and what actions you take in them
- Purchases or other transactions you make
- Hashtags you use
- The time, frequency and duration of your activities on our Products

[Friends, followers and other connections](#)

[App, browser and device information:](#)

- Device characteristics and device software
- What you're doing on your device (like whether our app is in the foreground or if your mouse is moving)
- Identifiers that tell your device apart from other users'
- Device signals
- Information you've shared through your device settings
- Information about the network you connect your device to, including your IP address

	<ul style="list-style-type: none"> Information from cookies and similar technologies <p>Information from Partners, vendors and third parties</p>
<p>Anonymizing your information</p> <p>In some cases, we anonymize information we have associated with you, such as your activity on and off our Products, and use the resulting information, for example, to provide and improve our Meta Products, including ads.</p>	<p>Your activity and information you provide:</p> <ul style="list-style-type: none"> 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 Metadata about content Types of content you view or interact with, and how you interact with it Apps and features you use, and what actions you take in them Purchases or other transactions you make Hashtags you use The time, frequency and duration of your activities on our Products <p>Friends, followers and other connections</p> <p>App, browser and device information:</p> <ul style="list-style-type: none"> Device characteristics and device software What you're doing on your device (like whether our app is in the foreground or if your mouse is moving)

	<ul style="list-style-type: none"> • Identifiers that tell your device apart from other users' • Device signals • Information you've shared through your device settings • Information about the network you connect your device to, including your IP address • Information from cookies and similar technologies <p>Information from Partners, vendors and third parties</p>
<p>Share information with others, including law enforcement and to respond to legal requests.</p> <p>See the "How do we respond to legal requests, prevent harm and promote safety and integrity?" section of the Meta Privacy Policy for more for information on when we share information with law enforcement and others.</p> <p>The categories of information we access, preserve, use and share depend on the specific circumstances. For example, responses to legal requests where not compelled by law will typically include limited information (such as contact details and login information).</p> <p>However, the information we process will depend on the purposes, which could include the following:</p> <ul style="list-style-type: none"> • In response to legal requests from third parties such as civil litigants, law enforcement and other government authorities 	<p>Your activity and information you provide:</p> <ul style="list-style-type: none"> • 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 • Metadata about content, subject to applicable law • Types of content you view or interact with, and how you interact with it • Apps and features you use, and what actions you take in them • Purchases or other transactions you make • Hashtags you use <p>Friends, followers and other connections</p>

- To comply with applicable law or legitimate legal purposes
- To promote the safety, security and integrity of Meta Companies, Meta Products, users, employees, property and the public

[Learn more](#) about how we promote safety, security and integrity.

app, browser and device information:

- Device characteristics and device software
- What you're doing on your device (like whether our app is in the foreground or if your mouse is moving)
- Identifiers that tell your device apart from other users'
- Device signals
- Information you've shared through your device settings
- Information about the network you connect your device to, including your IP address
- Information from cookies and similar technologies

[Information from Partners, vendors and third parties](#)

For processing information when the law requires it: Where we are under an obligation to disclose information such as, for example, if we receive a valid legal request for certain information such as a search warrant, we will access, preserve and/or share your information with regulators, law enforcement or others.

The way in which the information will be processed depends on the specific circumstances. See the "[How do we respond to legal requests, prevent harm and promote safety and integrity?](#)" section of the Meta Privacy Policy for more. "[Information for Law Enforcement Authorities](#)" provides information on the

The categories of information depend on the specific circumstances of each mandatory request or obligation. Only the information necessary to comply with the relevant legal obligation will be shared or otherwise processed. For example, for civil matters, this will typically include limited information (such as contact details and login information). However, depending on the circumstances it could include the following:

[Your activity and information you provide:](#)

operational guidelines law enforcement needs to follow.

- 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
- Messages you send and receive, including their content, subject to applicable law
- Metadata about content and messages, subject to applicable law
- Types of content you view or interact with, and how you interact with it
- Apps and features you use, and what actions you take in them
- Purchases or other transactions you make, including truncated credit card information
- Hashtags you use
- The time, frequency and duration of your activities on our Products

Friends, followers and other connections

App, browser and device information:

- Device characteristics and device software
- What you're doing on your device (like whether our app is in the foreground or if your mouse is moving)
- Identifiers that tell your device apart from other users'

	<ul style="list-style-type: none">• Device signals• Information you've shared through your device settings• Information about the network you connect your device to, including your IP address• Information from cookies and similar technologies <p>Information from Partners, vendors and third parties</p>
--	---

Exhibit K

facebook

Sign Up

Email or phone

Password

Forgot account?

- > Why do we use cookies?
- > Where do we use cookies?
- > Do other Companies use cookies in connection with the Meta Products?
- > How can you control your Information?

More Resources

· Printable Cookies Policy

· Data Policy

· Terms

· Facebook Ads Settings

· Privacy Basics

The Facebook company is now Meta. We've updated our Terms of Use, Data Policy, and Cookies Policy to reflect the new name on January 4, 2022. While our company name has changed, we are continuing to offer the same products, including the Facebook app from Meta. Our Data Policy and Terms of Service remain in effect, and this name change does not affect how we use or share data. [Learn more about Meta](#) and our vision for the metaverse.

Cookies & other storage technologies

Cookies are small pieces of text used to store information on web browsers. Cookies are used to store and receive identifiers and other information on computers, phones and other devices. Other technologies, including data that we store on your web browser or device, identifiers associated with your device and other software, are used for similar purposes. In this policy, we refer to all of these technologies as “cookies”.

We use cookies if you have a Facebook account, use the [Meta Products](#), including our website and apps, or visit other websites and apps that use the Meta Products (including the Like button). Cookies enable Meta to offer the Meta Products to you and to understand the information that we receive about you, including information about your use of other websites and apps, whether or not you are registered or logged in.

This policy explains how we use cookies and the choices you have. Except as otherwise stated in this policy, the [Data Policy](#) will apply to our processing of the data that we collect via cookies.



Return to top

Why do we use cookies?

Cookies help us provide, protect and improve the Meta Products, such as by

personalising content, tailoring and measuring ads, and providing a safer experience. The cookies that we use include session cookies, which are deleted when you close your browser, and persistent cookies, which stay in your browser until they expire or you delete them. While the cookies that we use may change from time to time as we improve and update the Meta Products, we use them for the following purposes:

Authentication

We use cookies to verify your account and determine when you're logged in so that we can make it easier for you to access the Meta Products and show you the appropriate experience and features.

For example: We use cookies to keep you logged in as you navigate between Facebook Pages. Cookies also help us remember your browser so you don't have to keep logging in to Facebook and so you can more easily log in to Facebook via third-party apps and websites. For example, we use the "c_user" and "xs" cookies, including for this purpose, which have a lifespan of 365 days.

Security, site and product integrity

We use cookies to help us keep your account, data and the Meta Products safe and secure.

For example: Cookies can help us identify and impose additional security measures when someone may be attempting to access a Facebook account without authorisation, for instance, by rapidly guessing different passwords. We also use cookies to store information that allows us to recover your account in the event that you forget your password or to require additional authentication if you tell us that your account has been hacked. This includes, for example, our "sb" and "dbln" cookies, which enable us to identify your browser securely, as well as "datr." "Datr" is a unique identifier for your browser that, amongst other things, helps us protect you from fraud. For example, it helps us identify trusted browsers where you have logged in before. "Datr" has a lifespan of two years.

We also use cookies to combat activity that violates our policies or otherwise degrades our ability to provide the Meta Products.

For example: Cookies help us fight spam and phishing attacks by enabling us to identify computers that are used to create large numbers of fake Facebook accounts. We also use cookies to detect computers infected with malware and to take steps to prevent them from causing further harm. Our "csrf" cookie, for example, helps us prevent cross-site request forgery attacks. The "datr" cookie also helps us to identify the browsers used by malicious actors and to prevent cyber-security attacks, such as a denial of service attack that could prevent you from accessing the Meta

Products. Cookies also help us prevent underage people from registering for Facebook accounts.

Advertising, recommendations, insights and measurement

We use cookies to help us show ads and to make recommendations for businesses and other organisations to people who may be interested in the products, services or causes they promote.

For example: Cookies allow us to help deliver ads to people who have previously visited a business's website, purchased its products or used its apps and to recommend products and services based on that activity. Cookies also allow us to limit the number of times that you see an ad so you don't see the same ad over and over again. For example, the "fr" cookie is used to deliver, measure and improve the relevancy of ads, with a lifespan of 90 days.

We also use cookies to help measure the performance of ad campaigns for businesses that use the Meta Products.

For example: We use cookies to count the number of times that an ad is shown and to calculate the cost of those ads. We also use cookies to measure how often people do things, such as make a purchase following an ad impression. For example, the "_fbp" cookie identifies browsers for the purposes of providing advertising and site analytics services and has a lifespan of 90 days.

Cookies help us serve and measure ads across different browsers and devices used by the same person.

For example: We can use cookies to prevent you from seeing the same ad over and over again across the different devices that you use.

Cookies also allow us to provide insights about the people who use the Meta Products, as well as the people who interact with the ads, websites and apps of our advertisers and the businesses that use the Meta Products.

For example: We use cookies to help businesses understand the kinds of people who like their Facebook Page or use their apps so that they can provide more relevant content and develop features that are likely to be interesting to their customers.

We also use cookies, such as our "oo" cookie, which has a lifespan of five years, to help you opt out of seeing ads from Meta based on your activity on third-party websites. [Learn more](#) about the information we receive, how we decide which ads to show you on and off the Meta Products and the controls that are available to you.

Site features and services

We use cookies to enable the functionality that helps us provide the Meta Products.

For example: Cookies help us store preferences, know when you've seen or interacted with Meta Products' content and provide you with customised content and experiences. For instance, cookies allow us to make suggestions to you and others, and to customise content on third-party sites that integrate our social plugins. If you are a Facebook Page administrator, cookies allow you to switch between posting from your personal Facebook account and the Facebook Page. We use cookies such as the session-based "presence" cookie to support your use of Messenger chat windows.

We also use cookies to help provide you with content relevant to your locale.

For example: We store information in a cookie that is placed on your browser or device so that you will see the site in your preferred language.

Performance

We use cookies to provide you with the best experience possible.

For example: Cookies help us route traffic between servers and understand how quickly Meta Products load for different people. Cookies also help us record the ratio and dimensions of your screen and windows and know whether you've enabled high-contrast mode, so that we can render our sites and apps correctly. For example, we set the "dpr" and "wd" cookies, each with a lifespan of 7 days, for purposes including to deliver an optimal experience for your device's screen.

Analytics and research

We use cookies to better understand how people use the Meta Products so that we can improve them.

For example: Cookies can help us understand how people use the Facebook service, analyse which parts of our Products people find most useful and engaging, and identify features that could be improved.

Third-party websites and apps

Our business partners may also choose to share information with Meta from cookies set in their own websites' domains, whether or not you have a Facebook account or are logged in. Specifically, cookies named `_fb` or `_fbp` may be set on the domain of the business partner whose site you're visiting. Unlike cookies that are set on Meta's own domains,

these cookies aren't accessible by Meta when you're on a site other than the one on which they were set, including when you are on one of our domains. They serve the same purposes as cookies set in Meta's own domain, which are to personalise content (including ads), measure ads, produce analytics and provide a safer experience, as set out in this Cookies Policy.



[Return to top](#)

Where do we use cookies?

We may place cookies on your computer or device and receive information stored in cookies when you use or visit:

- The [Meta Products](#);
- Products provided by other members of the [Meta Companies](#); and
- Websites and apps provided by other companies that use the Meta Products, including companies that incorporate Meta technologies into their websites and apps. Meta uses cookies and receives information when you visit those sites and apps, including [device information](#) and information about your activity, without any further action from you. This occurs whether or not you have a Facebook account or are logged in.



[Return to top](#)

Do other Companies use cookies in connection with the Meta Products?

Yes, other companies use cookies on the Meta Products to provide advertising, measurement, marketing and analytics services to us, and to provide certain features and improve our services for you.

For example, other companies' cookies help tailor ads off of Meta Products, measure their performance and effectiveness and support marketing and analytics. Certain features on the Meta Products use cookies from other companies to function, for example, certain maps, payment and security features. [Learn more](#) about the companies that use cookies on the Meta Products.

Third party companies also use cookies on their own sites and apps in connection

with the Meta Products. To understand how other companies use cookies, please review their policies.



[Return to top](#)

How can you control your Information?

We use cookies to help personalise and improve content and services, provide a safer experience and to show you useful and relevant ads on and off Meta Products. You can control how we use data to show you ads and more by using the tools described below.

If you have a Facebook account:

- You can use your [ad preferences](#) to learn why you're seeing a particular ad and control how we use information that we collect to show you ads.
- To show you better ads, we use data that advertisers and other partners provide us about your activity off Meta Company Products, including websites and apps. You can control whether we use this data to show you ads in your [ad settings](#).
- The Meta Audience Network is a way for advertisers to show you ads in apps and websites off the [Meta Company Products](#). One of the ways that Audience Network shows relevant ads is by using your ad preferences to determine which ads you may be interested in seeing. You can control this in your [ad settings](#).
- You can review your Off-Facebook activity, which is a summary of activity that businesses and organisations share with us about your interactions with them, such as visiting their apps or websites. They use our [business tools](#), such as Meta Pixel, to share this information with us. This helps us do things like give you a more personalised experience on Meta Products. Learn more [about off-Facebook activity](#), how we use it and how you can manage it.

Everyone:

You can opt out of seeing online interest-based ads from Meta and other participating companies through the [Digital Advertising Alliance](#) in the US, the [Digital Advertising Alliance of Canada](#) in Canada or the [European Interactive Digital Advertising Alliance](#) in Europe or through your mobile device settings, where available, using Android, iOS 13 or an earlier version of iOS. Please note that ad blockers and tools that restrict our cookie use may interfere with these controls.

More information about online advertising:

The advertising companies we work with generally use cookies and similar technologies as part of their services. To learn more about how advertisers generally use cookies and the choices they offer, you can review the following resources:

- [Digital Advertising Alliance](#)
- [Digital Advertising Alliance of Canada](#)
- [European Interactive Digital Advertising Alliance](#)

Browser cookie controls:

In addition, your browser or device may offer settings that allow you to choose whether browser cookies are set and to delete them. These controls vary by browser, and manufacturers may change both the settings they make available and how they work at any time. As of 23 June 2021, you may find additional information about the controls offered by popular browsers at the links below. Certain parts of the Meta Products may not work properly if you have disabled browser cookie use. Please be aware that these controls are distinct from the controls that we offer you.

- [Google Chrome](#)
- [Internet Explorer](#)
- [Firefox](#)
- [Safari](#)
- [Safari Mobile](#)
- [Opera](#)

Date of last revision: 5 October 2022

English (US) Español Français (France) 中文(简体) العربية Português (Brasil) Italiano 한국어 Deutsch हिन्दी 日本語 +

Sign Up Log In Messenger Facebook Lite Watch Places Games Marketplace Meta Pay Oculus Portal Instagram Bulletin Local Fundraisers
Services Voting Information Center Groups About Create Ad Create Page Developers Careers Privacy Cookies Ad choices Terms Help
Contact Uploading & Non-Users

Meta © 2022