

GIBSON, DUNN & CRUTCHER LLP
 LAUREN R. GOLDMAN (admitted *pro hac vice*)
 lgoldman@gibsondunn.com
 DARCY C. HARRIS (admitted *pro hac vice*)
 dharris@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

ANDREW M. KASABIAN, SBN 313210
 akasabian@gibsondunn.com
 3161 Michelson Drive
 Irvine, CA 92612 USA
 Telephone: (949) 451-3800
 Facsimile: (949) 451-4220

*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
 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

IN RE META PIXEL HEALTHCARE
 LITIGATION

This Document Relates To:
 All Actions

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

**DEFENDANT META PLATFORMS, INC.'S
 NOTICE OF MOTION AND MOTION TO
 DISMISS CONSOLIDATED CLASS ACTION
 COMPLAINT**

CLASS ACTION

Date: August 16, 2023
 Time: 2:00 p.m.
 Courtroom 2

HON. WILLIAM H. ORRICK

NOTICE OF MOTION AND MOTION

PLEASE TAKE NOTICE that on August 16, 2023, at 2:00 p.m., before the Honorable William Orrick of the United States District Court for the Northern District of California, Courtroom 2, 450 Golden Gate Avenue, San Francisco, CA 94102, Defendant Meta Platforms, Inc., will, and hereby does, move this Court pursuant to Federal Rule of Civil Procedure 12(b)(6) for an order dismissing the complaint with prejudice.

The motion is based upon this notice of motion; the memorandum of points and authorities in support thereof that follows; the proposed order filed concurrently herewith; the request for judicial notice and accompanying declaration; the pleadings, records, and papers on file in this action; oral argument of counsel; and any other matters properly before the Court.

STATEMENT OF ISSUES TO BE DECIDED

Should the complaint be dismissed under Rule 12(b)(6) for failure to state a claim?

TABLE OF CONTENTS

	<u>Page</u>
INTRODUCTION	1
BACKGROUND	2
A. Meta’s Pixel	2
B. Meta’s Terms	3
C. Plaintiffs’ Allegations	4
LEGAL STANDARD.....	4
ARGUMENT	5
A. Plaintiffs Do Not State a Claim Under the Federal Wiretap Act (Claim 3).....	5
1. Plaintiffs Fail to Adequately Plead Intent	5
2. The One-Party Consent Exemption Applies	6
3. Most Of The Allegedly Intercepted Information Was Not “Content”	9
B. The Complaint Does Not State a Claim Under CIPA (Claim 4)	10
1. CIPA Does Not Apply Extraterritorially	10
2. Plaintiffs Fail to Plausibly Allege Meta Had the Requisite Intent	10
3. Plaintiffs Do Not Plausibly Allege Data Was Sent From or Received in California.....	12
4. Plaintiffs Do Not Plausibly Allege that Meta Used a “Device”	12
C. Plaintiffs Do Not State a Constitutional Privacy (Claim 6) or Intrusion Upon Seclusion (Claim 5) Claim	13
D. Plaintiffs Fail to Plausibly Allege Violation of the CDAFA (Claim 12).....	15
E. The Complaint Does Not State Contract-Based Claims Against Meta (Claims 1 & 2)	16
F. Plaintiffs’ Requested Remedies and the Parties’ Agreements Doom the Unjust Enrichment Claim (Claim 13).....	19
G. Plaintiffs Have Not Plausibly Alleged a Negligence Per Se Cause of Action (Claim 7)	20
H. Plaintiffs Fail to Plausibly Allege a Trespass to Chattels Claim (Claim 8)	21
I. Plaintiffs Fail to Plausibly Allege A Statutory Larceny (Claim 11)	23
J. The UCL (Claim 9) and CLRA (Claim 10) Claims Fail on Multiple Counts.....	24

1 CONCLUSION 25

TABLE OF AUTHORITIES

Page(s)

CASES

<i>In re Apple Processor Litig.</i> , 2022 WL 2064975 (N.D. Cal. June 8, 2022)	20
<i>Armendariz v. Found. Health Psychare Servs., Inc.</i> , 24 Cal. 4th 83 (2000)	17
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009)	4
<i>Astra USA, Inc. v. Santa Clara Cty.</i> , 563 U.S. 110 (2011)	20
<i>Austin v. Atlina</i> , 2021 WL 6200679 (N.D. Cal. Dec. 22, 2021)	20
<i>Backhaut v. Apple, Inc.</i> , 74 F. Supp. 3d 1033 (N.D. Cal. 2014)	6
<i>Bass v. Facebook, Inc.</i> , 394 F. Supp. 3d 1024 (N.D. Cal. 2019)	17
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007)	4, 5
<i>Bellumini v. Citigroup, Inc.</i> , 2013 WL 3855589 (N.D. Cal. July 24, 2013)	13
<i>Cal. Serv. Station & Auto Repair Ass’n v. Am. Home Assurance Co.</i> , 62 Cal. App. 4th 1166 (1998)	20
<i>Cal. Soc’y of Anesthesiologists v. Brown</i> , 204 Cal. App. 4th 390 (2012)	11, 13
<i>Campbell v. Facebook Inc.</i> , 315 F.R.D. 250 (N.D. Cal. 2016)	9
<i>Campbell v. Facebook Inc.</i> , 77 F. Supp. 3d 836 (N.D. Cal. 2014)	24
<i>Caraccioli v. Facebook, Inc.</i> , 167 F. Supp. 3d 1056 (N.D. Cal. 2016)	17
<i>Careau & Co. v. Sec. Pac. Bus. Credit, Inc.</i> , 222 Cal. App. 3d 1371 (1990)	19

1	<i>Carreon v. Edwards</i> ,	
2	2022 WL 4664569 (E.D. Cal. Sept. 29, 2022).....	23
3	<i>Casillas v. Berkshire Hathaway Homestate Ins. Co.</i> ,	
4	79 Cal. App. 5th 755 (2022).....	22
5	<i>Chan v. Lund</i> ,	
6	188 Cal. App. 4th 1159 (2010).....	23
7	<i>Citizens of Humanity, LLC v. Costco Wholesale Corp.</i> ,	
8	171 Cal. App. 4th 1 (2009).....	23
9	<i>Cottle v. Plaid Inc.</i> ,	
10	536 F. Supp. 3d 461 (N.D. Cal. 2021)	15
11	<i>Custom Packaging Supply, Inc. v. Phillips</i> ,	
12	2015 WL 8334793 (C.D. Cal. Dec. 7, 2015)	15
13	<i>Darnaa, LLC v. Google LLC</i> ,	
14	756 F. App'x 674 (9th Cir. 2018)	17
15	<i>Day v. GEICO Cas. Co.</i> ,	
16	580 F. Supp. 3d 830 (N.D. Cal. 2022)	19
17	<i>Dent v. Nat'l Football League</i> ,	
18	902 F.3d 1109 (9th Cir. 2018).....	20
19	<i>Dfinity USA v. Bravick</i> ,	
20	2023 WL 2717252 (N.D. Cal. Mar. 29, 2023).....	23
21	<i>Doe v. Cal. Inst. of Tech.</i> ,	
22	2019 WL 8645652 (C.D. Cal. Aug. 13, 2019).....	17
23	<i>In re DoubleClick Inc. Priv. Litig.</i> ,	
24	154 F. Supp. 2d 497 (S.D.N.Y. 2001).....	7
25	<i>Durand v. U.S. Customs</i> ,	
26	163 F. App'x 542 (9th Cir. 2006)	24
27	<i>eBay, Inc. v. Bidder's Edge, Inc.</i> ,	
28	100 F. Supp. 2d 1058 (N.D. Cal. 2000)	21
	<i>In re Facebook, Inc. Internet Tracking Litig.</i> ,	
	956 F.3d 589 (9th Cir. 2020).....	5, 7, 14
	<i>In re Facebook, Inc. Sec. Litig.</i> ,	
	477 F. Supp. 3d 980 (N.D. Cal. 2020)	18
	<i>Federated Univ. Police Officers' Ass'n v. Regents of Univ. of Cal.</i> ,	
	2015 WL 13273308 (C.D. Cal. July 29, 2015)	5, 11

1	<i>Fidlar Techs. v. LPS Real Estate Data Sols., Inc.</i> ,	
2	810 F.3d 1075 (7th Cir. 2016).....	16
3	<i>Foley v. Interactive Data Corp.</i> ,	
4	47 Cal. 3d 654 (1988)	19
5	<i>Food Safety Net Servs. v. Eco Safe Sys. USA, Inc.</i> ,	
6	209 Cal. App. 4th 1118 (2012).....	17
7	<i>Gardiner v. Walmart, Inc.</i> ,	
8	2021 WL 4992539 (N.D. Cal. July 28, 2021).....	19
9	<i>Gonzales v. Uber Techs., Inc.</i> ,	
10	305 F. Supp. 3d 1078 (N.D. Cal. 2018)	15, 16
11	<i>In re Google Assistant Priv. Litig.</i> ,	
12	457 F. Supp. 3d 797 (N.D. Cal. 2020)	6
13	<i>In re Google Inc. Cookie Placement Consumer Priv. Litig.</i> ,	
14	806 F.3d 125 (3d Cir. 2015).....	8
15	<i>In re Google Inc. Gmail Litig.</i> ,	
16	2014 WL 1102660 (N.D. Cal. Mar. 18, 2014).....	7
17	<i>In re Google Location History Litig.</i> ,	
18	428 F. Supp. 3d 185 (N.D. Cal. 2019)	12
19	<i>In re Google, Inc. Priv. Policy Litig.</i> ,	
20	58 F. Supp. 3d 968 (N.D. Cal. 2014)	24
21	<i>Grafilo v. Wolfsohn</i> ,	
22	33 Cal. App. 5th 1024 (2019).....	13, 14
23	<i>Graham v. Noom, Inc.</i> ,	
24	533 F. Supp. 3d 823 (N.D. Cal. 2021)	9
25	<i>Guz v. Bechtel Nat'l Inc.</i> ,	
26	24 Cal. 4th 317 (2000)	19
27	<i>Hammerling v. Google LLC</i> ,	
28	2022 WL 17365255 (N.D. Cal. Dec. 1, 2022)	12
	<i>Hart v. TWC Prod. & Tech. LLC</i> ,	
	526 F. Supp. 3d 592 (N.D. Cal. 2021)	24
	<i>Haskins v. Symantec Corp.</i> ,	
	654 F. App'x 338 (9th Cir. 2016)	24
	<i>Hernandez v. Hillside, Inc.</i> ,	
	47 Cal. 4th 272 (2009)	13, 14

1	<i>Herskowitz v. Apple Inc.</i> ,	
2	940 F. Supp. 2d 1131 (N.D. Cal. 2013)	25
3	<i>Hill v. Nat'l Collegiate Athletic Ass'n</i> ,	
4	7 Cal. 4th 1 (1994)	14
5	<i>Intel Corp. v. Hamidi</i> ,	
6	30 Cal. 4th 1342 (2003)	21, 22
7	<i>In re iPhone Application Litig.</i> ,	
8	2011 WL 4403963 (N.D. Cal. Sept. 20, 2011)	16
9	<i>In re iPhone Application Litig.</i> ,	
10	844 F. Supp. 2d 1040 (N.D. Cal. 2012)	14, 22
11	<i>Johnson v. Honeywell Int'l Inc.</i> ,	
12	179 Cal. App. 4th 549 (2009).....	20
13	<i>Katz-Lacabe v. Oracle Am., Inc.</i> ,	
14	2023 WL 2838118 (N.D. Cal. Apr. 6, 2023)	7, 8, 9, 25
15	<i>Kearney v. Salomon Smith Barney, Inc.</i> ,	
16	39 Cal. 4th 95 (2006)	13
17	<i>Kellman v. Spokeo, Inc.</i> ,	
18	599 F. Supp. 3d 877 (N.D. Cal. 2022)	25
19	<i>Ladas v. Cal. State Auto. Ass'n</i> ,	
20	19 Cal. App. 4th 761 (1993).....	17, 18
21	<i>Lewis v. Superior Court</i> ,	
22	3 Cal. 5th 561 (2017)	13
23	<i>Loo v. Toyota Motor Sales, USA, Inc.</i> ,	
24	2019 WL 7753448 (C.D. Cal. Dec. 20, 2019)	25
25	<i>Lozano v. City of Los Angeles</i> ,	
26	73 Cal. App. 5th 711 (2022).....	11
27	<i>M Seven Sys. Ltd. v. Leap Wireless Int'l Inc.</i> ,	
28	2013 WL 12072526 (S.D. Cal. June 26, 2013).....	15
	<i>Microsoft Corp. v. Hon Hai Precision Indus. Co.</i> ,	
	2020 WL 5128629 (N.D. Cal. Aug. 31, 2020).....	19
	<i>Modisette v. Apple Inc.</i> ,	
	30 Cal. App. 5th 136 (2018).....	21
	<i>Moore v. Centrelake Med. Grp., Inc.</i> ,	
	83 Cal. App. 5th 515 (2022).....	21

1	<i>Moreno v. S.F. Bay Area Rapid Transit Dist.</i> ,	
2	2017 WL 6387764 (N.D. Cal. Dec. 14, 2017)	12, 13
3	<i>Nowak v. Xapo, Inc.</i> ,	
4	2020 WL 6822888 (N.D. Cal. Nov. 20, 2020).....	16
5	<i>O'Connor v. Uber Techs., Inc.</i> ,	
6	58 F. Supp. 3d 989 (N.D. Cal. 2014)	10, 18
7	<i>Oman v. Delta Air Lines, Inc.</i> ,	
8	889 F.3d 1075 (9th Cir. 2018).....	24
9	<i>Omega World Travel, Inc. v. Mummagraphics, Inc.</i> ,	
10	469 F.3d 348 (4th Cir. 2006).....	22
11	<i>Partti v. Palo Alto Med. Found. for Health Care, Rsch. & Educ., Inc.</i> ,	
12	2015 WL 6664477 (N.D. Cal. Nov. 2, 2015).....	19
13	<i>People v. Buchanan</i> ,	
14	26 Cal. App. 3d 274 (1972).....	11
15	<i>People v. Bustamante</i> ,	
16	57 Cal. App. 4th 693 (1997).....	13
17	<i>People v. Lyon</i> ,	
18	61 Cal. App. 5th 237 (2021).....	12
19	<i>People v. Superior Court (Smith)</i> ,	
20	70 Cal. 2d 123 (1969)	11
21	<i>Perkins v. LinkedIn Corp.</i> ,	
22	53 F. Supp. 3d 1190 (N.D. Cal. 2014)	24
23	<i>In re Pharmatrak, Inc.</i> ,	
24	329 F.3d 9 (1st Cir. 2003)	5
25	<i>Planned Parenthood Fed'n of Am., Inc. v. Newman</i> ,	
26	51 F.4th 1125 (9th Cir. 2022).....	7, 8
27	<i>Poublon v. C.H. Robinson Co.</i> ,	
28	846 F.3d 1251 (9th Cir. 2017).....	17
	<i>Pruchnicki v. Envision Healthcare Corp.</i> ,	
	845 F. App'x 613 (9th Cir. 2021)	25
	<i>Quiroz v. Seventh Ave. Ctr.</i> ,	
	140 Cal. App. 4th 1256 (2006).....	20
	<i>Rashdan v. Geissberger</i> ,	
	2011 WL 197957 (N.D. Cal. Jan. 14, 2011)	20

1	<i>Razuki v. Caliber Home Loans, Inc.</i> ,	
2	2018 WL 2761818 (S.D. Cal. June 8, 2018).....	14
3	<i>Rodriguez v. Google LLC</i> ,	
4	2021 WL 2026726 (N.D. Cal. May 21, 2021)	7
5	<i>Rosales v. City of Los Angeles</i> ,	
6	82 Cal. App. 4th 419 (2000).....	20
7	<i>Rosenfeld v. JPMorgan Chase Bank</i> ,	
8	732 F. Supp. 2d 952 (N.D. Cal. 2010)	19
9	<i>Rutherford Holdings, LLC v. Plaza Del Rey</i> ,	
10	223 Cal. App. 4th 221 (2014).....	19
11	<i>San Miguel v. HP Inc.</i> ,	
12	317 F. Supp. 3d 1075 (N.D. Cal. 2018)	16
13	<i>Sateriale v. R.J. Reynolds Tobacco Co.</i> ,	
14	697 F.3d 777 (9th Cir. 2012).....	17
15	<i>Seismic Reservoir 2020, Inc. v. Paulsson</i> ,	
16	785 F.3d 330 (9th Cir. 2015).....	5
17	<i>Sharma v. Volkswagen AG</i> ,	
18	524 F. Supp. 3d 891 (N.D. Cal. 2021)	20
19	<i>Siry Inv., L.P. v. Farkhondehpour</i> ,	
20	13 Cal. 5th 333 (2022)	23
21	<i>Skinner v. Tel-Drug, Inc.</i> ,	
22	2017 WL 1076376 (D. Ariz. Jan. 27, 2017).....	21
23	<i>Smith v. Facebook</i> ,	
24	262 F. Supp. 3d 943 (N.D. Cal. 2017)	14
25	<i>Smith v. Facebook, Inc.</i> ,	
26	745 F. App'x 8 (9th Cir. 2018)	6
27	<i>Sonner v. Premier Nutrition Corp.</i> ,	
28	971 F.3d 834 (9th Cir. 2020).....	20
	<i>Sullivan v. Oracle Corp.</i> ,	
	51 Cal. 4th 1191 (2011)	10, 24
	<i>Sussman v. Am. Broad. Cos.</i> ,	
	186 F.3d 1200 (9th Cir. 1999).....	8
	<i>Switzer v. Wood</i> ,	
	35 Cal. App. 5th 116 (2019).....	23

1	<i>Terpin v. AT&T Mobility, LLC</i> ,	
2	399 F. Supp. 3d 1035 (C.D. Cal. 2019).....	24
3	<i>United States v. Christensen</i> ,	
4	828 F.3d 763 (9th Cir. 2015).....	5, 6
5	<i>United States v. Forrester</i> ,	
6	512 F.3d 500 (9th Cir. 2008).....	14
7	<i>United States v. McTiernan</i> ,	
8	695 F.3d 882 (9th Cir. 2012).....	7
9	<i>Vartanian v. VW Credit, Inc.</i> ,	
10	2012 WL 12326334 (C.D. Cal. Feb. 22, 2012).....	11
11	<i>WhatsApp Inc. v. NSO Grp. Techs. Ltd.</i> ,	
12	472 F. Supp. 3d 649 (N.D. Cal. 2020)	22
13	<i>White v. Soc. Sec. Admin.</i> ,	
14	111 F. Supp. 3d 1041 (N.D. Cal. 2015)	15
15	<i>Williams v. Superior Court</i> ,	
16	3 Cal. 5th 531 (2017)	13
17	<i>Windham v. Davies</i> ,	
18	2015 WL 461628 (E.D. Cal. Feb. 3, 2015)	24
19	<i>In re Yahoo Mail Litig.</i> ,	
20	7 F. Supp. 3d 1016 (N.D. Cal. 2014)	13
21	<i>Yunker v. Pandora Media, Inc.</i> ,	
22	2013 WL 1282980 (N.D. Cal. Mar. 26, 2013).....	22
23	<i>Zapata Fonseca v. Goya Foods Inc.</i> ,	
24	2016 WL 4698942 (N.D. Cal. Sept. 8, 2016)	25
25	<i>Zaslow v. Kroenert</i> ,	
26	29 Cal. 2d 541 (1946)	22
27	<i>In re Zoom Video Commc'ns Inc. Priv. Litig.</i> ,	
28	525 F. Supp. 3d 1017 (N.D. Cal. 2021)	24
	<i>In re Zynga Priv. Litig.</i> ,	
	750 F.3d 1098 (9th Cir. 2014).....	9, 14
	STATUTES	
	18 U.S.C. § 2511	5, 7
	Cal. Bus. & Prof. Code § 17204	24

1 Cal. Penal Code § 484.....23, 24

2 Cal. Penal Code § 496.....23

3 Cal. Penal Code § 496.....23

4 Cal. Penal Code § 502.....15, 16

5 Cal. Penal Code § 630.....10

6 Cal. Penal Code § 631.....10, 11, 12

7 Cal. Penal Code § 632.....10, 12, 13

8

9 **TREATISES**

10 Restatement (Second) of Torts § 217.....22

11 **REGULATIONS**

12 45 C.F.R. § 160.10321

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

MEMORANDUM OF POINTS AND AUTHORITIES

INTRODUCTION

Plaintiffs’ rhetoric aside, this case concerns a relatively narrow issue: the allegation that healthcare providers decided to use a commonplace internet analytics tool to send sensitive health-related information to Meta that Meta never intended, and did not want, to receive. Meta acknowledges that the Court referred to this as a “potentially serious problem” in its order denying plaintiffs’ motion for a preliminary injunction, and Meta does not disagree; that is why it has built, and is constantly working to improve, the filtration systems that are designed to screen out potentially sensitive data when it is sent by web developers in violation of Meta’s policies.

Two undisputed points put plaintiffs’ claims in context.

First, there is nothing inherently unlawful or harmful about the pixel-based analytics technology at the heart of this case. This technology helps web developers measure certain actions users take on their websites—*e.g.*, what pages they view and what products they purchase—and use that information to grow their businesses and improve online user experiences. That ubiquitous and useful technology is offered by numerous companies (not just Meta) to web developers spanning numerous industries (not just healthcare). Meta’s version of this tool, the “Meta Pixel,” is of a piece with other companies’ offerings: Meta makes a generic bit of code publicly available, and third-party web developers can freely customize and install it to help them improve the online services they offer.

Second, web developers—not Meta—choose whether, where, and how they will use the Meta Pixel. Meta’s Business Tools Terms, which all web developers (healthcare provider or not) must agree to before integrating the Pixel code on their websites, (1) require web developers to confirm that they have the proper permissions and legal right to share any data they choose to send, and (2) tell web developers not to send *any* “health” or other sensitive information. Meta also has implemented a filtering mechanism to screen out potentially sensitive health data it detects, and to alert the developer so it can check how it has configured the Pixel and fix any issues. But it is ultimately the developer, not Meta, that controls the code on its own website and chooses what information to send. Plaintiffs attempt to distract the Court from these points by detailing the ways in which Meta allegedly encourages businesses in the healthcare sector to use its Business Tools, but these allegations miss the

point: These companies can use Meta’s Pixel without sending health information to Meta, and are expected to use the Pixel in compliance with Meta’s terms.

Plaintiffs have filed a grab-bag complaint asserting thirteen causes of action, ranging from “wiretap” violations to larceny to trespass. But *none* of those causes of action fits plaintiffs’ theory of the case—that *Meta* should be held liable for certain *healthcare providers*’ alleged misuse of a publicly available tool that Meta did not implement or configure on the providers’ websites. As a result, the claims fail for a host of reasons that this Court had no occasion to consider when it evaluated plaintiffs’ preliminary injunction motion.¹ Several of the claims—including the federal and state wiretapping claims—fail because plaintiffs do not allege the requisite intent by Meta to receive sensitive health information. Other claims fail because they are based on California laws that do not apply extraterritorially, and none of the plaintiffs is a California resident. Still others, like larceny and trespass, cannot be stretched to encompass the technology at issue and the facts alleged in this case. And many of the claims fail for *all* these reasons, plus element-specific reasons all their own.

The causes of action asserted in the complaint are poor vessels for the misguided theory of the case plaintiffs have advanced against Meta, and each of them should be dismissed.

BACKGROUND

A. Meta’s Pixel

This case centers on the Meta Pixel, “a free and publicly available piece of code that Meta allows third-party website developers” in “a range of industries” to “install on their websites.” Dkt. 159 at 2–3.² Developers can use the Pixel to (1) measure certain actions taken by users on the developers’ own sites and apps, and (2) assess and improve the effectiveness of the developers’ advertising. Compl. ¶¶ 101–03. The Pixel is “customizable,” and developers “choose the actions the

¹ Meta respectfully maintains that Facebook users consented to the data-sharing practices at issue in this case based on the clear and broad disclosures users must agree to when they create a Facebook account. *See* Dkt. 76 at 15–20. But in light of this Court’s contrary ruling in its order denying a preliminary injunction, Dkt. 159 at 12–17, this motion addresses the numerous other problems with plaintiffs’ claims.

² Plaintiffs allege the Pixel is used on applications as well, but it is used only on websites. *See, e.g.*, Compl. ¶¶ 6, 63, 242; Request for Judicial Notice (“RJN”) Ex. 6. Other “tracking tools,” like the SDK, are used on applications. *See* Dkt. 205 (Conditional Joint Motion to Relate); Compl. ¶¶ 1, 7.

Pixel will track and measure” on their websites. Compl. ¶ 44. While Meta provides instructions on how to install the Pixel, developers decide whether, how, where, and when to use it. Compl. ¶¶ 46–47.

B. Meta’s Terms

When users sign up for a Facebook account, they agree to Meta’s Terms of Service (the “Terms”), which govern the relationship between Meta and its users. Meta’s Terms govern the “use of Facebook, Messenger, and the other products, features, apps, services, technologies, and software” Meta offers. RJN Ex. 1 at 1. The Terms provide that Meta’s “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, indirect, exemplary, punitive, or incidental damages arising out of or related to these Terms or the Meta Products” (including the Meta Pixel). *Id.* at 7. Users also agree to Meta’s Privacy Policy, which notes that Meta “collect[s] and receive[s] information from” third parties, including information about “[w]ebsites you visit and cookie data, like through . . . the Meta Pixel.” RJN Ex. 4 at 6–7.

Third-party web developers that use Meta’s services—including the Meta Pixel tool—must agree to Meta’s Business Tools Terms and Commercial Terms. The Business Tools Terms require developers to “represent and warrant” that they “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.” RJN Ex. 2 at 2. Developers must also “represent and warrant that [they] have provided robust and sufficiently prominent notice to users regarding the Business Tool Data collection, sharing and usage,” including a “clear and prominent notice on each web page where [Meta] pixels are used that links to a clear explanation [of] . . . how users can opt-out of the collection and use of information for ad targeting.” *Id.* at 3–4.

To use the Pixel, developers must agree not to “share Business Tool Data . . . that [they] know or reasonably should know . . . includes health, financial information or other categories of sensitive information (including any information defined as sensitive under applicable laws, regulations and applicable industry guidelines).” *Id.* at 2. The Commercial Terms contain similar restrictions, and require developers to agree not to “send to [Meta], or use Meta [Pixel] to collect from people . . . health, financial, biometrics, or other categories of similarly sensitive information.” RJN Ex. 3 at 2.

C. Plaintiffs' Allegations

Plaintiffs are Maryland, Wisconsin, North Carolina, Ohio, and Missouri residents and Facebook users who communicate with their healthcare providers through the providers' websites. Compl. ¶¶ 24–28. They allege their providers incorporated the Meta Pixel onto their websites in a manner that resulted in the following information being sent to Meta: (1) that the plaintiffs were “communicating” with the providers' websites (without specifying what was being communicated); (2) that the plaintiffs clicked the login buttons on their providers' websites; (3) that two of the plaintiffs had “previously visited” webpages about breast health and medical records; (4) the plaintiffs' IP addresses; and (5) cookies and browser attributes. Compl. ¶¶ 79, 81–82. As a result, plaintiffs allege the providers sent information to Meta revealing their identity, that they logged into their providers' patient portals, and the pages they visited before logging in. Compl. ¶¶ 80, 82.

Plaintiffs allege Meta encourages “health” entities to use its tools, including the Meta Pixel, and to advertise on Meta's platforms. Compl. ¶ 126; *see* Compl. ¶¶ 129–46. Plaintiffs also allege Meta does not verify that developers have consent to share the data they send. Compl. ¶¶ 115–16. But the complaint acknowledges Meta has a filtration system to detect and filter out potentially sensitive health data, including “information that web developers have no right to send.” Compl. ¶¶ 118, 125.

Plaintiffs bring thirteen claims against Meta, seeking monetary and injunctive relief on behalf of themselves and a putative class of “[a]ll Facebook users whose health information was obtained by Meta from their health care provider or covered entity.” Compl. ¶ 274.

LEGAL STANDARD

A complaint must “contain sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). On a motion to dismiss, the Court must first separate the complaint's legal conclusions—which are disregarded—from its factual allegations. *Id.* at 678–79. The remaining factual allegations must “raise a right to relief above the speculative level.” *Twombly*, 550 U.S. at 555. If the complaint pleads facts that are “‘merely consistent with’ a defendant's liability, it ‘stops short of the line between possibility and plausibility of entitlement to relief.’” *Iqbal*, 556 U.S.

at 678 (quoting *Twombly*, 550 U.S. at 557). Claims also may be dismissed based on a dispositive issue of law. *Seismic Reservoir 2020, Inc. v. Paulsson*, 785 F.3d 330, 335 (9th Cir. 2015).

ARGUMENT

A. Plaintiffs Do Not State a Claim Under the Federal Wiretap Act (Claim 3)

“The Wiretap Act prohibits the unauthorized ‘interception’ of an ‘electronic communication.’” *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 606–07 (9th Cir. 2020) (quoting 18 U.S.C. § 2511(1)(a)–(e)). Plaintiffs must plausibly allege that Meta “(1) intentionally (2) intercepted (3) the contents of (4) plaintiffs’ electronic communications (5) using a device.” Dkt. 159 at 17. And because the Wiretap Act is a one-party consent statute, Meta is not liable if *any* party to a communication consented to sharing it, unless Meta obtained the information for “the purpose of committing any criminal or tortious act.” 18 U.S.C. § 2511(2)(d). Plaintiffs’ claim fails to meet these requirements.

1. Plaintiffs Fail to Adequately Plead Intent

Plaintiffs’ Wiretap Act claim fails because they do not allege that Meta *intentionally*—that is, “purposefully and deliberately”—intercepted their sensitive health information. *United States v. Christensen*, 828 F.3d 763, 774 (9th Cir. 2015).³ Where a party obtains information “as a result of accident or mistake,” *id.*, or an alleged interception is “the product of inadvertence,” *In re Pharmatrak, Inc.*, 329 F.3d 9, 23 (1st Cir. 2003), the intent element is not satisfied. Rather, the defendant must have “acted *consciously and deliberately* with the goal of intercepting wire communications.” *Christensen*, 828 F.3d at 775 (emphasis added). Even a party who sells and installs a recording system, and provides instructions for its use, is not liable for another party’s misuse of that system. *See Federated Univ. Police Officers’ Ass’n v. Regents of Univ. of Cal.*, 2015 WL 13273308, at *7 (C.D. Cal. July 29, 2015). So too here: Meta’s actions in making a standard Internet tool “free and publicly available,” Compl. ¶ 39, do not give rise to liability whenever a web developer misuses that tool.

Plaintiffs assert that Meta “intentionally intercepted” their health information, *see* Compl. ¶¶ 335, 358, but offer no factual allegations in support. Developers—not Meta—control whether, how, and where to use the pixel tool. *See* Compl. ¶¶ 39, 44–46. Meta contractually *prohibits* web developers

³ At the preliminary injunction stage, Meta did “not dispute that the intentional or interception elements are met.” Dkt. 159 at 18. The Court has thus not yet assessed Meta’s “intent” arguments.

from sending potentially sensitive information. *See* RJN Ex. 2 at 2. Plaintiffs acknowledge Meta’s efforts to “create[] a ‘filter to detect data sent through the Pixel’ that Meta ‘categorizes as potentially sensitive data, including health data.’” Compl. ¶ 118 (quoting Wooldridge Decl. ¶ 8); *see* Compl. ¶ 125. And they invoke Meta’s “public descriptions of systems it already has in place” and Meta’s position that it “d[oes] not want health information.” Compl. ¶¶ 148–49. Taken separately or together, these allegations affirmatively *negate* any suggestion that Meta’s “purpose[]” is to receive sensitive health information. *Christensen*, 828 F.3d at 774.

Plaintiffs allege that Meta encourages “health” companies to use the pixel tool and advertise with Meta. *See, e.g.*, Compl. ¶¶ 126–27, 131, 134–46, 231, 242–43. But those allegations do not plausibly suggest any intent to receive *sensitive* health information for a simple and commonsense reason: Just like any other entity that may possess some sensitive information about its customers, healthcare providers can use the pixel tool in any number of perfectly legitimate ways without sharing sensitive data. *E.g.*, *Smith v. Facebook, Inc.*, 745 F. App’x 8, 8–9 (9th Cir. 2018). Given the many legitimate uses of the Meta Pixel on health-related websites, the alleged existence of a Meta “Health” marketing division does not plausibly suggest any unlawful intent to receive sensitive data.⁴

The Wiretap Act claim must be dismissed due to lack of intent.

2. The One-Party Consent Exemption Applies

The Wiretap Act claim also must be dismissed because at least one party (the providers who configured the Meta Pixel on their website) consented—indeed, affirmatively chose—to share information with Meta, and Meta lacked any criminal or tortious purpose in receiving that information.

The Wiretap Act does not impose liability “where *one* of the parties to the communication has given prior consent” unless the “communication [was] intercepted for the purpose of committing any

⁴ Some courts have allowed Wiretap Act claims to proceed beyond the pleadings stage where “a defendant is aware of the defect causing the interception but takes no remedial action.” *In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d 797, 815 (N.D. Cal. 2020); *Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033, 1044 (N.D. Cal. 2014). These decisions are inconsistent with the Ninth Circuit’s decision in *Christensen*, because mere knowledge of a defect does not constitute “act[ing] consciously and deliberately with the goal of intercepting wire communications.” 828 F.3d at 774. But even if those cases were correctly decided, they would not help plaintiffs here, because plaintiffs do not plausibly allege that Meta declined to take any remedial action. Rather, Meta *has* taken action to remedy the conduct of developers who violate these policies by creating a filtration system that aims to detect and filter out even *potentially* sensitive health data. *See* Compl. ¶¶ 118, 125(c).

1 criminal or tortious act.” 18 U.S.C. § 2511(2)(d) (emphasis added); *see In re Facebook*, 956 F.3d at
 2 607. The healthcare providers “who configured the Pixel on their websites presumably consented to
 3 Meta’s receipt of the information.” Dkt. 159 at 20; *see Katz-Lacabe v. Oracle Am., Inc.*, 2023 WL
 4 2838118, at *10 (N.D. Cal. Apr. 6, 2023). To state a claim, then, plaintiffs must plausibly allege that
 5 Meta intercepted their information “for the purpose of committing” a crime or tort. 18 U.S.C.
 6 § 2511(2)(d). They fail to do so.

7 The requisite criminal or tortious purpose “must be *separate and independent* from the act of
 8 the recording.” *Planned Parenthood Fed’n of Am., Inc. v. Newman*, 51 F.4th 1125, 1136 (9th Cir.
 9 2022) (emphasis added). Plaintiffs had to allege both that Meta intended to *intercept* their
 10 communications (*see supra* at 5–6), and that Meta intended to *use* their data to commit an independent
 11 crime or tort. “[T]he focus is *not* upon whether the interception itself violated [the] law; it is upon
 12 whether the *purpose* for the interception—its intended use—was criminal or tortious.” *Planned*
 13 *Parenthood*, 51 F.4th at 1136; *see also United States v. McTiernan*, 695 F.3d 882, 890 (9th Cir. 2012)
 14 (courts “look to the purpose” and ask whether it “directly facilitates” some *other* “criminal conduct”).
 15 And the defendant must have intended to use the recording to commit a crime or tort “[a]t the time of
 16 the recording.” *Planned Parenthood*, 51 F.4th at 1136.

17 Plaintiffs allege that Meta’s purpose in making its pixel tool available to developers is to help
 18 companies in a wide range of industries improve their online advertising and services. *See, e.g.*, Compl.
 19 ¶¶ 39–42. Acting for commercial gain is not a criminal or tortious purpose. *See* Dkt. 159 at 21; *see*
 20 *also Katz-Lacabe*, 2023 WL 2838118, at *10; *Rodriguez v. Google LLC*, 2021 WL 2026726, at *6 n.8
 21 (N.D. Cal. May 21, 2021); *In re DoubleClick Inc. Priv. Litig.*, 154 F. Supp. 2d 497, 518 (S.D.N.Y.
 22 2001); *In re Google Inc. Gmail Litig.*, 2014 WL 1102660, at *18 n.13 (N.D. Cal. Mar. 18, 2014). In
 23 *Katz-Lacabe*, the plaintiffs alleged that the defendant used cookies and tracking pixels to collect
 24 personal data and then “to aggregate and synchronize the collected data to perform ‘identity
 25 resolution,’” which the defendant traded and sold to third-party data brokers and clients for profit. 2023
 26 WL 2838118, at *1–2, *10. The crime-tort exception did not apply because the defendant’s purpose
 27 was commercial profit, not to commit a tort, and the court dismissed the Wiretap Act claim. *Id.* at *10.

1 So too here. Plaintiffs allege that Meta received sensitive data through the Meta Pixel to
 2 enhance its advertising and “to make money,” not “to perpetuate torts on millions of Internet users.”
 3 *Katz-Lacabe*, 2023 WL 2838118, at *10. Meta’s policies prohibiting developers from sending sensitive
 4 health information confirm that Meta did not intend to use the Pixel to commit a crime or tort. And
 5 Meta’s attempts to filter out any potentially sensitive health information that developers send in
 6 violation of its terms drive the point home—Meta did not have any “criminal or tortious purpose at the
 7 time the [interception] was made.” *Planned Parenthood*, 51 F.4th at 1136; *see* Compl. ¶¶ 118, 125(c).

8 Plaintiffs present a laundry list of various crimes and torts that they allege Meta committed by
 9 receiving their sensitive health data. Compl. ¶ 347. Not one of those alleged purposes is “separate and
 10 independent from the act of recording.” *Planned Parenthood*, 51 F.4th at 1136; *Sussman v. Am. Broad.*
 11 *Cos.*, 186 F.3d 1200, 1202 (9th Cir. 1999). Rather, the crimes and torts plaintiffs tick off “occur[]
 12 through the act of interception itself.” *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806
 13 F.3d 125, 145 (3d Cir. 2015). Plaintiffs concede as much when they allege “[i]n acquiring the contents
 14 of Plaintiffs’ and Class Members’ communications relating to patient portals, appointments, and phone
 15 calls, Meta had a purpose that was tortious, criminal, and designed to violate state constitution and
 16 statutory provisions,” and then list thirteen laws Meta allegedly violated through that acquisition.
 17 Compl. ¶ 347 (emphasis added). Plaintiffs thus allege that Meta’s purpose was to commit a tort or
 18 crime *through the act of interception itself*.

19 A closer look at these allegations confirms that plaintiffs do not allege an independent crime or
 20 tort. Subparagraphs 347(a) through (c) concern the alleged “unauthorized acquisition of individually
 21 identifiable health information” under HIPAA—*i.e.*, “the act of interception itself.” *In re Google Inc.*
 22 *Cookie Placement*, 806 F.3d at 145. Subparagraphs (d) through (h), (j), and (k) list several of plaintiffs’
 23 other causes of action, all of which also concern Meta’s alleged interception of information.
 24 Subparagraph (i) alleges “[v]iolations of various state health privacy statutes,” including California’s
 25 “Confidentiality of Medical Information Act,” “Consumer Privacy Protection Act,” and “Consumer
 26 Privacy Act,” without further explanation. And subparagraph (l) restates two federal wire fraud
 27 provisions, which concern devising a scheme to defraud another out of money or property without any
 28 further explanation; but plaintiffs do not allege that Meta defrauded them out of money or property.

1 See Compl. ¶ 348; *infra* at 24. Because plaintiffs have not alleged that Meta intercepted their sensitive
 2 information for the *purpose* of committing a crime or tort “separate and independent” of receipt itself,
 3 the crime-tort exception is inapplicable.

4 **3. Most Of The Allegedly Intercepted Information Was Not “Content”**

5 The Wiretap Act requires interception of “the content of a communication”—“the intended
 6 message conveyed by the communication, and [not] record information regarding the characteristics of
 7 the message that is generated in the course of the communication.” *In re Zynga Priv. Litig.*, 750 F.3d
 8 1098, 1106 (9th Cir. 2014). Plaintiffs allege Meta intercepted: (1) the name of SubscribedButtonClick
 9 events; (2) previously visited provider websites; and (3) IP addresses and other identifiers that can
 10 identify plaintiffs and their devices. Compl. ¶¶ 79(c)–(h), 81(c)–(h), 339. This Court has stated that
 11 the name of SubscribedButtonClick events may be “content” that was intercepted, Dkt. 159 at 18–19,
 12 but none of the remaining items constitutes content.

13 *First*, any information used to identify plaintiffs or their devices, including IP address, is record
 14 information, not content. Record information is data “generated in the course of the communication,”
 15 including the “name, address and subscriber number or identity of a subscriber or customer”; and the
 16 “origin, length, and time of a call, or geolocation data.” *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823,
 17 833 (N.D. Cal. 2021) (quoting *Zynga*, 750 F.3d at 1106). “There is no language in [the Wiretap Act]
 18 equating ‘contents’ with personally identifiable information.” *Zynga*, 750 F.3d at 1107.

19 *Second*, plaintiffs do not allege that Meta received any content pertaining to websites they
 20 previously visited. URLs that merely contain the “address of the webpage the user was viewing before
 21 clicking on [an] icon” are not, without more, content. *Campbell v. Facebook Inc.*, 315 F.R.D. 250, 265
 22 (N.D. Cal. 2016); *see Katz-Lacabe*, 2023 WL 2838118, at *9. This Court has observed that *some* URL
 23 information, such as that identified in the Smith Declaration, can be sufficiently descriptive to qualify
 24 as “content” where it includes both path and query strings. *See* Dkt. 159 at 19 & n.10. But the Smith
 25 Declaration is not tethered to the named plaintiffs’ claims: plaintiffs do not allege that Meta intercepted
 26 URLs that contain query strings. Instead, they allege, *e.g.*, that Meta learned that John Doe I
 27 communicated with MedStar via “www.MedStarHealth.org” and “[h]e had previously visited a
 28 MedStar page about breast health.” Compl. ¶ 79(a), (e). The screenshots accompanying paragraphs

79 and 81 of the complaint confirm the lack of any “content”; there are no query strings and neither the referer header nor the destination header contain “content” information under *Zynga*. Thus, the named plaintiffs’ allegations regarding information that Meta received about *their own* previously visited websites do not plausibly establish Meta received any content.⁵

B. The Complaint Does Not State a Claim Under CIPA (Claim 4)

Plaintiffs also bring a claim under the California Invasion of Privacy Act (CIPA), a state analogue to the Wiretap Act. That claim also suffers from multiple deficiencies that compel dismissal.

1. CIPA Does Not Apply Extraterritorially

Plaintiffs are Maryland, Wisconsin, North Carolina, Ohio, and Missouri residents who do not allege that the alleged misconduct took place in California. *See* Compl. ¶¶ 24–28. “Under California law, a presumption exists against the extraterritorial application [of] state law.” *O’Connor v. Uber Techs., Inc.*, 58 F. Supp. 3d 989, 1004 (N.D. Cal. 2014). Courts must “presume the Legislature did not intend a statute to be operative, with respect to occurrences outside the state, . . . unless such intention is clearly expressed or reasonably to be inferred from the language of the act or from its purpose, subject matter or history.” *Sullivan v. Oracle Corp.*, 51 Cal. 4th 1191, 1207 (2011) (citations omitted).

Nothing in CIPA displaces the presumption. CIPA’s intent is “to protect the right of privacy of the *people of this state*.” Cal. Penal Code § 630 (emphasis added). Had the Legislature intended to provide for extraterritorial application, it would have done so expressly—as it has in other statutes. Plaintiffs are not “people of this state,” and none of their providers is based in California. Nor do they allege that they accessed their providers’ websites in California, that they were injured in California, or that any wiretapping or eavesdropping took place in California. They cannot bring a CIPA claim.

2. Plaintiffs Fail to Plausibly Allege Meta Had the Requisite Intent

Sections 631(a) and 632(a) of CIPA both require a showing that the defendant *intentionally* engaged in wiretapping or eavesdropping. Cal. Penal Code §§ 631(a), 632(a). Plaintiffs must plead “specific factual circumstances that make plausible [Meta’s] intent to record a confidential

⁵ Plaintiffs allege additional “contents” in conclusory fashion. *See* Compl. ¶ 338. But again, those generic references are not tethered to any allegations about the named plaintiffs’ data. Compl. ¶¶ 79, 81; *see* Compl. ¶ 82.

communication.” *Vartanian v. VW Credit, Inc.*, 2012 WL 12326334, at *2 (C.D. Cal. Feb. 22, 2012). They have not done so.

Section 632(a)’s intent requirement is satisfied only if the plaintiff proves “the person using the recording equipment [did] so with the *purpose or desire* of recording a confidential conversation, or with the *knowledge to a substantial certainty* that his use of the equipment will result in the recordation of a confidential conversation.” *People v. Superior Court (Smith)*, 70 Cal. 2d 123, 134 (1969) (emphases added). It is not enough to intend to use a recording device; instead, a defendant must intend to use it *for an impermissible purpose*. This rule “provides effective protection against ‘eavesdroppers’ without penalizing the innocent use of recording equipment.” *Id.* Section 631(a) likewise requires that a defendant “intentionally tap[ped]” or “willfully and without the consent of all parties to the communication . . . reads, or attempts to read . . . the contents or meaning of any message, report or communication.” Cal. Penal Code § 631(a). The intent requirement must be interpreted the same way across both provisions. *Cal. Soc’y of Anesthesiologists v. Brown*, 204 Cal. App. 4th 390, 403 (2012).

Because CIPA requires an *affirmative desire* to eavesdrop on or intercept a confidential communication, the “deploy[ment of] recording devices that *might* happen” to record such information is insufficient. *Lozano v. City of Los Angeles*, 73 Cal. App. 5th 711, 727–28 (2022) (quoting *Smith*, 70 Cal. 2d at 134); *see also, e.g., Federated Univ. Police Officers’ Ass’n v. Regents of Univ. of Cal.*, 2015 WL 13273308, at *10 (C.D. Cal. July 29, 2015) (no liability for selling and installing a recording device). The unintentional or inadvertent receipt of information “by chance” likewise cannot support a CIPA claim. *Smith*, 70 Cal. 2d at 133. “[A] person might intend to record the calls of wild birds on a game reserve and at the same time accidentally pick up the confidential discussions of two poachers. To hold the birdwatcher punishable under [CIPA] for such a fortuitous recording would be absurd.” *Id.*; *see also People v. Buchanan*, 26 Cal. App. 3d 274, 287–88 (1972) (finding no intent where switchboard operator “inadvertent[ly]” overheard a telephone conversation).

Pixels are a useful, legal, ubiquitous internet analytics tool, and creating a tool and making it freely available to others is not the intentional conduct that CIPA prohibits. *See Federated Univ.*, 2015 WL 13273308, at *10. Nor does it plausibly establish that Meta knew with “substantial certainty” that it would be receiving potentially sensitive health-related data from providers. *See Smith*, 70 Cal. 2d at

1 134. Given that Meta took steps to filter out such information as well as the undisputed fact that Meta
 2 contractually barred developers from sending it such data, there is no basis to conclude that Meta
 3 *intended* to receive any potentially sensitive health information.

4 **3. Plaintiffs Do Not Plausibly Allege Data Was Sent From or Received in California**

5 Section 631(a) applies only when a person “reads, or attempts to read, or to learn the contents
 6 or meaning of any message, report, or communication” while it is “being sent from, or received at any
 7 place *within this state*.” Cal. Penal Code § 631(a) (emphasis added). Plaintiffs do not plausibly allege
 8 any data was sent from or received in California. *See supra* at 10. They merely allege, in conclusory
 9 fashion, that Meta “designed and effectuated its scheme to track the patient communications at issue
 10 here from California.” Compl. ¶ 369. Another judge in this district recently dismissed a CIPA claim
 11 against Google on this precise basis, holding it was not enough to allege that “events and conduct giving
 12 rise to Plaintiffs’ claims occurred in California” or that “California is the state from which [defendant]’s
 13 alleged misconduct emanated.” *Hammerling v. Google LLC*, 2022 WL 17365255, at *11 (N.D. Cal.
 14 Dec. 1, 2022). Nor is the presence of Meta’s headquarters in California, *see* Compl. ¶¶ 29, 369, enough
 15 to demonstrate where plaintiffs’ information was actually “sent from” or “received.” Cal. Penal Code
 16 § 631(a); *Hammerling*, 2022 WL 17365255, at *11.

17 **4. Plaintiffs Do Not Plausibly Allege that Meta Used a “Device”**

18 The section 632(a) claim also fails because plaintiffs do not plausibly allege Meta used any
 19 “electronic amplifying or recording device[s].” Cal. Penal Code § 632(a). A device under CIPA is “a
 20 thing made or adapted for a particular purpose, especially a piece of mechanical or electronic
 21 equipment.” *Moreno v. S.F. Bay Area Rapid Transit Dist.*, 2017 WL 6387764, at *5 (N.D. Cal. Dec.
 22 14, 2017). CIPA therefore applies to *devices* such as video recorders, *People v. Lyon*, 61 Cal. App. 5th
 23 237, 245 (2021), but not software or apps, *In re Google Location History Litig.*, 428 F. Supp. 3d 185,
 24 193 (N.D. Cal. 2019) (Google Maps); *Moreno*, 2017 WL 6387764, at *5 (mobile software). The CIPA
 25 claim does not identify any “device” Meta allegedly used, and the “devices” identified in the Wiretap
 26 Act claim do not qualify for devices under CIPA. *See* Compl. ¶ 340. The Pixel and cookies do not
 27 qualify because CIPA does not apply to software. *See In re Google Location History*, 428 F. Supp. 3d
 28

at 193; *Moreno*, 2017 WL 6387764, at *5.⁶ The remaining “devices” do not qualify because they are not used to “record [any] confidential communication.” Cal. Penal Code § 632(a).

C. Plaintiffs Do Not State a Constitutional Privacy (Claim 6) or Intrusion Upon Seclusion (Claim 5) Claim

The “California Constitution and the common law both set a high bar for an invasion of privacy claim,” *Bellumini v. Citigroup, Inc.*, 2013 WL 3855589, at *6 (N.D. Cal. July 24, 2013); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1038 (N.D. Cal. 2014), and courts typically assess them together. *Hernandez v. Hillside, Inc.*, 47 Cal. 4th 272, 288 (2009). A plaintiff “must demonstrate (1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy.” *Lewis v. Superior Court*, 3 Cal. 5th 561, 571 (2017) (quotation marks omitted). Plaintiffs fail to plausibly allege these claims.

The California Constitution Does Not Apply Extraterritorially. The fact that none of the plaintiffs is a California resident dooms their constitutional claim. *See supra* at 10; Compl. ¶¶ 24–28. The presumption against extraterritoriality applies to California Constitution claims, *see People v. Bustamante*, 57 Cal. App. 4th 693, 699 n.5 (1997), and the privacy provision’s purpose is to protect “Californians.” *Williams v. Superior Court*, 3 Cal. 5th 531, 552 (2017); *Kearney v. Salomon Smith Barney, Inc.*, 39 Cal. 4th 95, 125 (2006).

No Legally Protected Interest. This Court previously held that plaintiffs had a legally protected interest in “[c]ommunications made in the context of a patient-medical provider relationship.” Dkt. 159 at 24–25. But critically, plaintiffs’ complaint does not plausibly allege such communications within the meaning of *this* cause of action. A constitutionally protected informational privacy interest is limited to “*sensitive and confidential* information,” *In re Yahoo*, 7 F. Supp. 3d at 1041, such as “symptoms, family history, diagnoses, test results and other intimate details concerning treatment,” *Grafilo v. Wolfsohn*, 33 Cal. App. 5th 1024, 1034 (2019) (quoting *Lewis*, 3 Cal. 5th at 575).

There are no specific allegations about the kinds of data Meta allegedly received about John Doe II or Jane Does II and III. Compl. ¶ 82. John Doe I’s and Jane Doe I’s allegations are likewise

⁶ Although *Moreno* and *In re Google Location History* concern a separate provision of CIPA that addresses electronic tracking devices, the term “device” should be interpreted the same way across the statute. *See Brown*, 204 Cal. App. 4th at 403.

very limited. These plaintiffs allege that Meta received information allowing it to infer that (1) they were using a device associated with a particular Facebook account and (2) they attempted to log in to their providers' patient portals. *See* Compl. ¶¶ 79–81. This data is not sensitive information on the order of medical history or “intimate details concerning treatment.” *Grafilo*, 33 Cal. App. 5th at 1034. Neither plaintiff alleges that Meta received medical histories, profiles, or indeed any information about their treatment. *Id.* They have not plausibly alleged any “[c]ommunications made in the context of a patient-medical provider relationship” in which they had a legally protected interest. Dkt. 159 at 24.⁷

No Sufficiently Serious Invasion. These claims also fail because plaintiffs do not allege an invasion that is “sufficiently serious” as to “constitute an egregious breach of the social norms underlying the privacy right.” *Hill v. Nat’l Collegiate Athletic Ass’n*, 7 Cal. 4th 1, 37 (1994). This Court previously suggested that Meta did “behave[] egregiously,” comparing Meta’s conduct to the theft of personal information. Dkt. 159 at 26–27. But again, the named plaintiffs do not allege that Meta obtained such information about *them*, much less that it did so with the intent of committing theft.

Meta’s efforts to filter potentially sensitive health information are also highly “relevant in the ‘highly offensive’” inquiry, Dkt. 159 at 26–27 (quoting *In re Facebook Internet Tracking Litig.*, 956 F.3d at 606). “[N]o cause of action will lie for accidental, misguided, or excusable acts of overstepping upon legitimate privacy rights.” *Hernandez*, 47 Cal. 4th at 295. “[N]egligent conduct” or conduct such as implementing “low-budget security measures,” even with an “absolute disregard of [their] consequences,” and even if they result in the loss of sensitive information like social security numbers, is *not* sufficiently egregious. *See Razuki v. Caliber Home Loans, Inc.*, 2018 WL 2761818, at *2 (S.D. Cal. June 8, 2018); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012).

Plaintiffs’ failure to plausibly allege that Meta “disseminat[ed] or misuse[d]” any sensitive health information further undermines any assertion that Meta’s alleged breach was “sufficiently

⁷ The rest of the information allegedly sent to Meta—IP address, browser information, and previously accessed webpages, *see* Compl. ¶ 81(e)–(f), (h)—does not constitute communications, let alone legally protected communications. This information is record information and automatically generated information such as non-descriptive URLs. *See supra* at 9–10. This distinguishes the alleged information here from “detailed URLs” discussed in the preliminary injunction order. Dkt. 159 at 25. This information does not qualify as legally protected information. *See United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008); *Zynga*, 750 F.3d at 1108; *see also Smith v. Facebook*, 262 F. Supp. 3d 943, 954–55 (N.D. Cal. 2017) (URLs containing general health information are not protected health information).

serious.” *Hill*, 7 Cal. 4th at 35. Plaintiffs simply allege they have “an interest in precluding the dissemination and misuse of their health information by Meta,” without plausibly alleging *how* Meta disseminated or misused their information. Compl. ¶ 393. “Without more allegations as to what, if anything, [Meta improperly] did with this information, [plaintiffs] ha[ve] not plausibly alleged a serious invasion of privacy.” *Gonzales v. Uber Techs., Inc.*, 305 F. Supp. 3d 1078, 1092–93 (N.D. Cal. 2018); *see White v. Soc. Sec. Admin.*, 111 F. Supp. 3d 1041, 1053 (N.D. Cal. 2015).

D. Plaintiffs Fail to Plausibly Allege Violation of the CDAFA (Claim 12)

The California Comprehensive Data Access and Fraud Act (CDAFA) is a misfit for this case. CDAFA is an “anti-hacking statute intended to prohibit the unauthorized use of any computer system for improper or illegitimate purpose.” *Custom Packaging Supply, Inc. v. Phillips*, 2015 WL 8334793, at *3 (C.D. Cal. Dec. 7, 2015). But this is not a “hacking” case. Plaintiffs allege Meta “knowingly accessed, used, and caused to be used” plaintiffs’ devices through the Pixel and _fbp cookie in violation of several sections of the CDAFA, Compl. ¶¶ 478–79, but that shoehorn attempt falls flat.

First, CDAFA does not apply extraterritorially. CDAFA was promulgated to ensure the well-being of individuals and entities “*within this state* that lawfully utilize” computers, computer systems, and computer data. Cal. Penal Code § 502(a) (emphasis added); *see id.* § 502(e)(3), (f). “[T]he California Penal Code”—including CDAFA—is therefore not “intended to reach . . . extra-territorial activity.” *M Seven Sys. Ltd. v. Leap Wireless Int’l Inc.*, 2013 WL 12072526, at *3 (S.D. Cal. June 26, 2013). And plaintiffs fail to allege any misconduct in California. *See supra* at 10, 12.

Second, CDAFA requires alleged “damage or loss by reason of a violation,” which plaintiffs do not and cannot allege. Cal. Penal Code § 502(e)(1). Plaintiffs generically allege they were precluded from communicating with their providers using their devices, *see* Compl. ¶ 484(a), (c), but this is not a damage or loss contemplated by CDAFA. *See Cottle v. Plaid Inc.*, 536 F. Supp. 3d 461, 488 (N.D. Cal. 2021). Plaintiffs’ further claim that they were damaged by “[t]he diminution in value of their protected health information,” Compl. ¶ 484(b), is insufficient because “loss of the value of their data” is not “‘damage or loss’ within the meaning of the CDAFA,” *Cottle*, 536 F. Supp. 3d at 488.

Third, plaintiffs fail to plausibly allege Meta violated sections 502(c)(1)–(3) and (6)–(8) of CDAFA. *Gonzales*, 305 F. Supp. 3d at 1090. “[W]hether there is liability under § 502 requires an

analysis of the specific ‘acts’ that are alleged to constitute an offense and whether there was ‘permission’ to engage in those acts.” *San Miguel v. HP Inc.*, 317 F. Supp. 3d 1075, 1087 (N.D. Cal. 2018). And because CDAFA claims “sound[] in fraud,” they are “subject to Rule 9(b)’s [heightened] pleading standard.” *Nowak v. Xapo, Inc.*, 2020 WL 6822888, at *5 (N.D. Cal. Nov. 20, 2020). These “boilerplate allegations do not survive Rule 8,” let alone Rule 9(b). *Gonzales*, 305 F. Supp. 3d at 1090.

Each of these provisions requires “*knowing*” conduct—*knowingly* accessing computer systems, taking data, using computer services, providing a means of accessing a computer system, or introducing a computer contaminant. Plaintiffs do not plausibly allege any knowing conduct. *See supra* at 5–6.

Plaintiffs also fail to plausibly allege violations of sections 502(c)(1) and (c)(8) on additional grounds. To allege a violation of section 502(c)(1), plaintiffs must plausibly allege Meta accessed or used data either (1) in furtherance of a scheme to defraud or (2) to wrongfully control or obtain money, property, or data. Cal. Penal Code § 502(c)(1). But they do not allege any such scheme nor do they plausibly allege that Meta wrongfully controlled or obtained any data, because they do not allege that Meta engaged in intentional wrongdoing. *See supra* at 5–6.

Plaintiffs’ claim based on violation of section 502(c)(8) fails because they have not plausibly alleged that Meta “introduce[d] any computer contaminant.” Cal. Penal Code § 502(c)(8). CDAFA is “aimed at ‘viruses or worms,’ and other malware that usurps the normal operation of the computer or computer system.” *In re iPhone Application Litig.*, 2011 WL 4403963, at *13 (N.D. Cal. Sept. 20, 2011). Plaintiffs allege that Pixel “is designed to, and does, self-propagate to contaminate users’ computers, computer systems, and computer networks,” Compl. ¶ 477, but there are no allegations that the Pixel “impair[s] the integrity or availability of” systems, *Fidlar Techs. v. LPS Real Estate Data Sols., Inc.*, 810 F.3d 1075, 1084 (7th Cir. 2016). Nor is the Pixel anything like “viruses or worms.” *In re iPhone Application Litig.*, 2011 WL 4403963, at *13. Finally, Meta did not “introduce” anything: developers customize and decide whether and where to implement the Pixel. Compl. ¶¶ 44, 46–47.

E. The Complaint Does Not State Contract-Based Claims Against Meta (Claims 1 & 2)

Plaintiffs bring claims for breach of contract and the implied covenant of good faith and fair dealing, predicated on alleged violations of Meta’s Terms and Privacy Policy. Those claims are barred by Meta’s limitation-of-liability provision and are meritless in any event.

1 **1.** Meta’s Terms contain a clear limitation-of-liability provision: “[Meta]’s liability shall
 2 be limited to the fullest extent permitted by applicable law, and under no circumstance will we be liable
 3 to you for any lost profits, revenues, information, or data, or consequential, special, indirect, exemplary,
 4 punitive, or incidental damages arising out of or related to these Terms or the Meta Products.” RJN
 5 Ex. 1 at 7. California law enforces such clauses “unless [they are] unconscionable.” *Food Safety Net*
 6 *Servs. v. Eco Safe Sys. USA, Inc.*, 209 Cal. App. 4th 1118, 1126 (2012).

7 This clause is not unconscionable. “[U]nconscionability has both a ‘procedural’ and a
 8 ‘substantive’ element, the former focusing on ‘oppression’ or ‘surprise’ due to unequal bargaining
 9 power, the latter on ‘overly harsh’ or ‘one-sided’ results.” *Armendariz v. Found. Health Psychare*
 10 *Servs., Inc.*, 24 Cal. 4th 83, 114 (2000). Procedurally, there is no “rule that an adhesion contract is per
 11 se unconscionable.” *Poublon v. C.H. Robinson Co.*, 846 F.3d 1251, 1261–62 (9th Cir. 2017). Judge
 12 Alsup has held that because “the procedure followed by Facebook was fair,” the limitation-of-liability
 13 “clause was not buried,” and it “contain[s] clear enough language,” the clause is not unconscionable.
 14 *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1037–38 (N.D. Cal. 2019). Substantively, these clauses
 15 are routinely enforced where, as here, the complained-of conduct involves third parties. *See, e.g.*,
 16 *Caraccioli v. Facebook, Inc.*, 167 F. Supp. 3d 1056, 1063 (N.D. Cal. 2016), *aff’d*, 700 F. App’x 588,
 17 590 (9th Cir. 2017); *Darnaa, LLC v. Google LLC*, 756 F. App’x 674, 675 (9th Cir. 2018).

18 **2.** Plaintiffs’ contract claims also fail on the merits. Plaintiffs fail to identify “sufficiently
 19 definite” provisions that allow the court “to ascertain the parties’ obligations and to determine whether
 20 those obligations have been performed or breached.” *Sateriale v. R.J. Reynolds Tobacco Co.*, 697 F.3d
 21 777, 789 (9th Cir. 2012). A “promise must be definite enough that a court can determine the scope of
 22 the duty[,] and the limits of performance must be sufficiently defined.” *Ladas v. Cal. State Auto. Ass’n*,
 23 19 Cal. App. 4th 761, 770 (1993). The complaint contains a chart that purports to outline four
 24 “promises and Meta’s breach.” Compl. ¶ 312. These provisions are not sufficiently definite to support
 25 a contract claim. *Doe v. Cal. Inst. of Tech.*, 2019 WL 8645652, at *5 (C.D. Cal. Aug. 13, 2019)
 26 (provisions stating investigators would be impartial, trained in relevant issues, not retaliate for reporting
 27 misconduct, and not tolerate intentional false reporting, were “not ‘sufficiently definite’”).
 28

Plaintiffs principally rely on Meta’s commitment to “require” partners to have the right to share user information with Meta. But that alleged promise does not allow “a court [to] determine the scope of [Meta’s] duty” or the “limits of performance,” *Ladas*, 19 Cal. App. 4th at 770. The Court’s prior statement that “‘require’ is susceptible to multiple meanings” confirms that this statement is not sufficiently definite to provide a basis for a breach of contract claim. Dkt. 159 at 17. Analyzing a similar provision, Judge Davila held that the “data policy only represents that it would ‘require’” certain conduct, which does not provide an actionable contract claim as Meta “makes no guarantees about how [it] would enforce that requirement.” *In re Facebook, Inc. Sec. Litig.*, 477 F. Supp. 3d 980, 1013 (N.D. Cal. 2020). The other provisions all discuss methods by which Meta *detects* “potential misuse,” but state nothing about the scope of those duties or what (if any) affirmative obligations Meta may have if potential misuse is discovered. That Meta will “take appropriate action” if there is potential misuse, Compl. ¶ 312, fails to remedy this problem: to the extent plaintiffs claim Meta’s filters do not constitute “appropriate action,” the terms they cite are not “sufficiently definite” to evaluate that claim.

3. Even if these provisions were sufficiently definite to support a contract claim, plaintiffs have failed to allege that they were breached. Plaintiffs simply quote the contract and say Meta “has not” or “does not” adhere to its provisions. Their claim that Meta does not “require Partners to have the right to . . . share [users’] information before giving it to” Meta is undermined by the Business Tools Terms and Commercial Terms, which *do* require exactly that. RJN Ex. 2 at 2, Ex. 3 at 2. Plaintiffs contend this contractual requirement is insufficient, but they supply no basis to demand performance over and above that or Meta’s filtration efforts. *See Ladas*, 19 Cal. App. 4th at 770.

4. Plaintiffs’ tagalong claims fail as duplicative. *First*, plaintiffs allege that “an implied contract also exists between Meta and Plaintiffs . . . that Meta will not conspire with others to violate Plaintiffs’ . . . legal rights to privacy in their individually identifiable health information.” Compl. ¶ 313. But plaintiffs acknowledge that there is a valid contract between the parties, and an implied contract claim “cannot lie where there [is] a valid and express contract covering the same subject matter.” *O’Connor*, 58 F. Supp. 3d at 999–1000.

Second, plaintiffs allege Meta breached the implied covenant of good faith and fair dealing by failing to take sufficient affirmative steps and “appropriate action” to ensure providers had the right to

collect and share their data. *See, e.g.*, Compl. ¶¶ 323–27. But an implied covenant “cannot impose substantive duties or limits on the contracting parties beyond those incorporated in the specific terms of their agreement.” *Rosenfeld v. JPMorgan Chase Bank*, 732 F. Supp. 2d 952, 968 (N.D. Cal. 2010); *see Guz v. Bechtel Nat’l Inc.*, 24 Cal. 4th 317, 349–50 (2000); *Partti v. Palo Alto Med. Found. for Health Care, Rsch. & Educ., Inc.*, 2015 WL 6664477, at *5 (N.D. Cal. Nov. 2, 2015). An implied covenant “is limited to assuring compliance with the *express terms* of the contract, and cannot be extended to create obligations not contemplated by the contract.” *Microsoft Corp. v. Hon Hai Precision Indus. Co.*, 2020 WL 5128629, at *8 (N.D. Cal. Aug. 31, 2020); *see Foley v. Interactive Data Corp.*, 47 Cal. 3d 654, 690 (1988). Plaintiffs cannot rewrite the terms of their contract with Meta to impose obligations the agreement itself does not impose.

Further, even if this claim extended beyond the contract claim, plaintiffs have not plausibly alleged that Meta “fail[ed] or refus[ed] to discharge contractual responsibilities . . . by a conscious and deliberate act,” as required for an implied-covenant claim. *Careau & Co. v. Sec. Pac. Bus. Credit, Inc.*, 222 Cal. App. 3d 1371, 1395 (1990). Their sole suggestion—that “Meta actively solicited [providers’] further disclosures and advertising revenue,” Compl. ¶¶ 325–26—is irrelevant. That Meta allegedly encourages *all* companies, including health-related companies, *e.g.*, Compl. ¶¶ 41–42, 116, to use the Pixel does not plausibly establish that Meta deliberately refused to discharge contractual responsibilities or take “appropriate action” against providers who did not have permission to share data with Meta. Compl. ¶¶ 323–27; *see supra* at 3, 6.

F. Plaintiffs’ Requested Remedies and the Parties’ Agreements Doom the Unjust Enrichment Claim (Claim 13)

Plaintiffs also bring a cursory unjust enrichment claim, which fails for at least two reasons.

First, plaintiffs cannot pursue an unjust enrichment claim as a quasi-contract cause of action where, as here, a “valid express contract covering the same subject matter” exists. *Rutherford Holdings, LLC v. Plaza Del Rey*, 223 Cal. App. 4th 221, 231 (2014); *see* Compl. ¶¶ 304, 312, 490. Given that there is no “dispute over validity or enforceability” of Meta’s Terms and Privacy Policy, dismissal “with prejudice is appropriate.” *Day v. GEICO Cas. Co.*, 580 F. Supp. 3d 830, 841 (N.D. Cal. 2022); *Gardiner v. Walmart, Inc.*, 2021 WL 4992539, at *8 (N.D. Cal. July 28, 2021).

Second, plaintiffs fail to plead that they “lack[] an adequate remedy at law” to redress any alleged past harm, as they must to bring equitable claims like unjust enrichment. *Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 844 (9th Cir. 2020); *see also Sharma v. Volkswagen AG*, 524 F. Supp. 3d 891, 907 (N.D. Cal. 2021); *In re Apple Processor Litig.*, 2022 WL 2064975, at *11–12 (N.D. Cal. June 8, 2022). While the court’s preliminary injunction order suggested that the “allegedly ongoing disclosure of plaintiffs’” potentially sensitive information “cannot be remedied by damages,” Dkt. 159 at 28 (emphasis added), that says nothing about whether plaintiffs lack an adequate remedy for any alleged past harm. Because plaintiffs do not allege that legal remedies cannot make them whole for any alleged past violations, this claim must be dismissed.

G. Plaintiffs Have Not Plausibly Alleged a Negligence Per Se Cause of Action (Claim 7)

Plaintiffs’ “claim” for negligence per se must be dismissed. “[N]egligence per se is a doctrine, not an independent cause of action,” *Dent v. Nat’l Football League*, 902 F.3d 1109, 1117 (9th Cir. 2018), and it does not create a “private right of action for violation of a statute,” *Johnson v. Honeywell Int’l Inc.*, 179 Cal. App. 4th 549, 556 (2009). Negligence per se simply establishes a presumption of negligence if the defendant (1) violated a statute; (2) the violation caused injury; (3) the injury “resulted from an occurrence the nature of which the statute . . . was designed to prevent”; and (4) the individual harmed was part of the class of persons the statute was designed to protect. *Quiroz v. Seventh Ave. Ctr.*, 140 Cal. App. 4th 1256, 1285 (2006). But plaintiffs still must plausibly allege an underlying negligence cause of action, which requires breach of a duty of care that caused injury. *See Cal. Serv. Station & Auto Repair Ass’n v. Am. Home Assurance Co.*, 62 Cal. App. 4th 1166, 1177 (1998); *Rosales v. City of Los Angeles*, 82 Cal. App. 4th 419, 430 (2000). Plaintiffs satisfy neither requirement here.

First, plaintiffs have not plausibly alleged Meta had a duty to comply with HIPAA. Compl. ¶ 403.⁸ “An alleged HIPAA violation cannot form the basis of a negligence claim,” because HIPAA has no private right of action. *Austin v. Atlina*, 2021 WL 6200679, at *3 (N.D. Cal. Dec. 22, 2021); *see Astra USA, Inc. v. Santa Clara Cty.*, 563 U.S. 110, 117 (2011); *Moore v. Centrelake Med. Grp.*,

⁸ Outside of HIPAA, plaintiffs allege no applicable duty beyond a cursory reference to “all applicable statutes and regulations,” Compl. ¶ 403, but such a reference does not “provide [Meta] with ‘fair notice’ of the basis of [plaintiffs’] claim,” *Rashdan v. Geissberger*, 2011 WL 197957, at *10 (N.D. Cal. Jan. 14, 2011) (finding it insufficient to incorporate preceding paragraphs).

1 *Inc.*, 83 Cal. App. 5th 515, 535–36 (2022). To allow “HIPAA regulations to define per se the duty and
 2 liability for breach” would allow plaintiffs to conjure up such a right despite Congress’ decision not to
 3 create one. *Skinner v. Tel-Drug, Inc.*, 2017 WL 1076376, at *3 (D. Ariz. Jan. 27, 2017). HIPAA does
 4 not apply to Meta in any event. Meta is not a covered entity; nor is it a covered “business associate,”
 5 which is an entity that “creates, receives, maintains, or transmits protected health information for a
 6 function or activity regulated by [HIPAA].” 45 C.F.R. § 160.103. Plaintiffs do not allege that Meta
 7 fits the bill, let alone that it does so for their specific providers.

8 *Second*, plaintiffs have not plausibly alleged causation. They make a single conclusory
 9 allegation that their purported injuries were “a direct and proximate result of Meta’s violations of
 10 HIPAA,” Compl. ¶ 412, but their other allegations undermine this claim. Plaintiffs admit that no data
 11 is sent to Meta unless third parties choose to install the Pixel. Compl. ¶ 39. Plaintiffs further admit
 12 that third parties control the nature of the data sent via the “customizable” Pixel. Compl. ¶ 44. Plaintiffs
 13 allege Meta encouraged *installation* of the Pixel, Compl. ¶ 41, but they do not plausibly claim Meta
 14 encouraged sending HIPAA-protected data through the Pixel. *See* Compl. ¶¶ 71–74, 138–46. By
 15 plaintiffs’ own account, Meta “did nothing more than create the condition that made Plaintiffs’ injuries
 16 possible,” and is therefore not legally responsible for those injuries. *Modisette v. Apple Inc.*, 30 Cal.
 17 App. 5th 136, 154 (2018). To the contrary, the only affirmative actions Meta arguably takes are
 18 designed to *avoid* receipt of health information. RJN Ex. 2 at 2, Ex. 4 at 7.

19 **H. Plaintiffs Fail to Plausibly Allege a Trespass to Chattels Claim (Claim 8)**

20 Plaintiffs’ trespass claim is another basic misfit for the facts of this case. Plaintiffs say Meta
 21 trespassed on their “computing devices” when the Meta Pixel caused the “_fbp” cookie to be placed
 22 on their devices, rendering them “useless for exchanging private communications.” Compl. ¶¶ 424–
 23 25. For plaintiffs to prevail on this claim, they must plausibly allege that “(1) defendant intentionally
 24 and without authorization interfered with plaintiff’s possessory interest in the computer system; and
 25 (2) defendant’s unauthorized use proximately resulted in damage to plaintiff.” *eBay, Inc. v. Bidder’s*
 26 *Edge, Inc.*, 100 F. Supp. 2d 1058, 1069–70 (N.D. Cal. 2000); *see also Intel Corp. v. Hamidi*, 30 Cal.
 27 4th 1342, 1364 (2003). The complaint satisfies neither prong.

1 *First*, for the same reasons discussed *supra* at 5–6, plaintiffs have not plausibly alleged Meta
 2 had the requisite intent. Intent to trespass “is present when an act is done for the purpose of using or
 3 otherwise intermeddling with a chattel or with knowledge that such an intermeddling will, to a
 4 substantial certainty, result from the act.” Restatement (Second) of Torts § 217 cmt. c (2023 update).
 5 Moreover, plaintiffs plainly consented to cookies being placed on their computers when they accepted
 6 the Cookies Policy. *See* RJN 5 at 1, 3, 5–6.

7 *Second*, plaintiffs fail to allege that Meta “damage[d] the recipient computer []or impair[ed] its
 8 functioning.” *Intel*, 30 Cal. 4th at 1364. Plaintiffs allege their computing devices “derive substantial
 9 value from their ability to facilitate communications with their health care providers or covered
 10 entities,” Compl. ¶ 423, but do not allege that this was the “intended function[]” of their devices or that
 11 any communication was “significantly reduc[ed].” *In re iPhone Application Litig.*, 844 F. Supp. 2d at
 12 1069. For this claim plaintiffs must, and do not, allege a *technical* impairment, like “significantly
 13 reducing [a device’s] memory and processing power.” *Intel*, 30 Cal. 4th at 1356; *see also In re iPhone*
 14 *Application Litig.*, 844 F. Supp. 2d at 1069 (allegations of reduced storage, bandwidth, and battery life
 15 did not state a claim because they did not amount to a “significant reduction in service constituting an
 16 interference with the intended functioning of the system”); *WhatsApp Inc. v. NSO Grp. Techs. Ltd.*,
 17 472 F. Supp. 3d 649, 684–85 (N.D. Cal. 2020). “[T]respass to chattels [does] not lie to protect interests
 18 in privacy”; plaintiffs cannot “convert privacy harms into property harms.” *Casillas v. Berkshire*
 19 *Hathaway Homestate Ins. Co.*, 79 Cal. App. 5th 755, 765 (2022).

20 Nor can Plaintiffs rely simply on the use of the Pixel and alleged “installation” of the _fbp
 21 cookie, *see* Compl. ¶ 424, because “installat[ion] of unwanted code” that “consume[s] portions of the
 22 memory on [a plaintiff’s] mobile device” does not suffice for a trespass claim. *Yunker v. Pandora*
 23 *Media, Inc.*, 2013 WL 1282980, at *15–16 (N.D. Cal. Mar. 26, 2013). Plaintiffs’ trespass claim also
 24 cannot be premised on nominal damages, *see* Compl. ¶ 426(a), because trespass allows one to “recover
 25 only the *actual* damages suffered by reason of the impairment of the property or the loss of its use.”
 26 *Zaslow v. Kroenert*, 29 Cal. 2d 541, 551 (1946). In the absence of any actual damage or dispossession,
 27 a trespass claim will not lie. *See Intel*, 30 Cal. 4th at 308; *Omega World Travel, Inc. v.*
 28 *Mummagraphics, Inc.*, 469 F.3d 348, 359 (4th Cir. 2006). Plaintiffs do not allege that Meta impaired

the functioning of their devices, and their claim that they were no longer able to send *private* communications is an improper attempt to convert a claimed privacy interest into a property interest.

I. Plaintiffs Fail to Plausibly Allege A Statutory Larceny (Claim 11)

Plaintiffs assert a “statutory larceny” cause of action premised on Penal Code sections 484 and 496, alleging that Meta “stole, took, and fraudulently appropriated” plaintiffs’ “individually identifiable health information” and “knew” that this “information was stolen.” Compl. ¶¶ 460–62. But larceny is another basic misfit for the facts of this case.

First, statutory larceny does not apply extraterritorially and plaintiffs do not allege any theft occurred in California. *See supra* at 10, 15. There is no “clearly expressed” intent for section 496 to apply outside California, so California’s presumption against extraterritoriality bars the application of section 496 here. *Dfinity USA v. Bravick*, 2023 WL 2717252, at *4–5 (N.D. Cal. Mar. 29, 2023).

Second, plaintiffs have not plausibly alleged a violation of section 496. They would have to allege “that (i) the property was stolen or obtained in a manner constituting theft, (ii) the defendant knew the property was so stolen or obtained, and (iii) the defendant received or had possession of the stolen property.” *Switzer v. Wood*, 35 Cal. App. 5th 116, 126 (2019). Plaintiffs do not plausibly allege anything was stolen or taken in a manner constituting theft. Plaintiffs freely provided information to their providers. While those providers may have provided some information to Meta allegedly in violation of plaintiffs’ *privacy* rights, that does not establish any information was stolen. And even if plaintiffs could prevail on their fraud- or contract-based claims, that is not enough because “a misrepresentation or breach of contract made innocently or inadvertently does not amount to theft.” *Carreon v. Edwards*, 2022 WL 4664569, at *5 (E.D. Cal. Sept. 29, 2022); *see Siry Inv., L.P. v. Farkhondehpour*, 13 Cal. 5th 333, 361–62 (2022).

Nor do plaintiffs plausibly allege that Meta *knew* plaintiffs’ information was stolen. As explained above, *see supra* at 5–6, plaintiffs have not sufficiently alleged that Meta intended to receive potentially sensitive health information; even assuming some information slipped through Meta’s filter, plaintiffs have not alleged any “knowing purchase, receipt, concealment or withholding of stolen property.” *Citizens of Humanity, LLC v. Costco Wholesale Corp.*, 171 Cal. App. 4th 1, 18 (2009); *see Chan v. Lund*, 188 Cal. App. 4th 1159, 1172 (2010).

1 *Third*, to the extent plaintiffs assert this claim under section 484, it must be dismissed because
 2 section 484 does not provide a private cause of action. *See Durand v. U.S. Customs*, 163 F. App'x 542,
 3 544–45 (9th Cir. 2006); *Windham v. Davies*, 2015 WL 461628, at *6 (E.D. Cal. Feb. 3, 2015).

4 **J. The UCL (Claim 9) and CLRA (Claim 10) Claims Fail on Multiple Counts**

5 Plaintiffs' UCL and injunction-only CLRA claims fail for a long list of reasons.

6 *First*, neither claim applies extraterritorially, and the complaint contains no plausible
 7 allegations showing that “the liability-creating conduct” occurred in California. *Oman v. Delta Air*
 8 *Lines, Inc.*, 889 F.3d 1075, 1079 (9th Cir. 2018); *see supra* at 10, 15. “[T]he presumption against
 9 extraterritoriality applies to the UCL in full force.” *Sullivan*, 51 Cal. 4th at 1207. And there is no
 10 “clearly expressed” intent that the CLRA should apply extraterritorially. *Id.*; *Terpin v. AT&T Mobility,*
 11 *LLC*, 399 F. Supp. 3d 1035, 1047–48 (C.D. Cal. 2019) (CLRA does not apply extraterritorially).

12 *Second*, both claims fail because plaintiffs do “not allege that [they] read and relied on a specific
 13 misrepresentation.” *Haskins v. Symantec Corp.*, 654 F. App'x 338, 339 (9th Cir. 2016); *see Perkins v.*
 14 *LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1219–20 (N.D. Cal. 2014). Actual reliance requires that plaintiffs
 15 plausibly allege that they *read* the alleged misrepresentations—which plaintiffs characterize as the
 16 “requirement that businesses have the right to collect, use, and share Plaintiffs’ . . . data before
 17 providing any data to Meta.” Compl. ¶ 433. Plaintiffs fail to allege they read anything, let alone “when
 18 and where they” viewed any alleged misrepresentation. *In re Zoom Video Commc'ns Inc. Priv. Litig.*,
 19 525 F. Supp. 3d 1017, 1045–46 (N.D. Cal. 2021). That is “fatal” to their claims. *In re Google, Inc.*
 20 *Priv. Policy Litig.*, 58 F. Supp. 3d 968, 982 (N.D. Cal. 2014).

21 *Third*, the UCL claim fails because plaintiffs do not plausibly allege the loss of “money or
 22 property.” Cal. Bus. & Prof. Code § 17204. Their conclusory statements that they “have suffered
 23 injuries in fact” are insufficient when their only factual allegation is that Meta’s “sale” of “individually
 24 identifiable and health data” to unspecified entities has “diminished its value to Plaintiffs.” Compl.
 25 ¶ 437; *see Hart v. TWC Prod. & Tech. LLC*, 526 F. Supp. 3d 592, 603 (N.D. Cal. 2021) (external value
 26 of data does not establish loss of money or property); *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836,
 27 849 (N.D. Cal. 2014). And “the ‘mere misappropriation of personal information’ does not establish
 28

compensable damages,” either. *Pruchnicki v. Envision Healthcare Corp.*, 845 F. App’x 613, 615 (9th Cir. 2021); *see Katz-Lacabe*, 2023 WL 2838118, at *8.

Fourth, plaintiffs’ request for restitution under the UCL fails because plaintiffs allege an adequate remedy at law. They will be unable to plausibly allege otherwise through amendment because the claims are all premised on the same factual predicates. Where plaintiffs’ equitable claims for past harms are based on the same factual predicates as their legal claims, they are not “true alternative theor[ies] of relief but rather [are] duplicative.” *Loo v. Toyota Motor Sales, USA, Inc.*, 2019 WL 7753448, at *13 (C.D. Cal. Dec. 20, 2019) (dismissing with prejudice); *see Zapata Fonseca v. Goya Foods Inc.*, 2016 WL 4698942, at *7 (N.D. Cal. Sept. 8, 2016). Nowhere do plaintiffs explain why the damages they seek for other claims are inadequate. *See supra* at 20.

Fifth, plaintiffs’ claim under the “unlawful” prong of the UCL fails because it is predicated on the same theories underlying their other claims, making the failure of those underlying theories fatal. *See* Compl. ¶ 432; *Kellman v. Spokeo, Inc.*, 599 F. Supp. 3d 877, 896 & n.5 (N.D. Cal. 2022).

Sixth, plaintiffs’ claim under the “unfair” prong of the UCL fails because they do not satisfy either the “balancing” or “tethering” tests. As to the “balancing” test, plaintiffs have not identified which conduct or acts by Meta were “immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers,” particularly since the complaint acknowledges that Meta takes substantial steps to prevent receipt of potentially sensitive information. *See Herskowitz v. Apple Inc.*, 940 F. Supp. 2d 1131, 1145–46 (N.D. Cal. 2013). Nor do they plead *any* facts alleging that any harm outweighs the utility of Meta’s conduct. *Id.*; *see supra* at 2–3 (explaining the beneficial and legitimate uses of the Pixel). Plaintiffs also fail to plausibly allege Meta engaged in a practice that “threatens an incipient violation of an antitrust law, or violates the policy or spirit of one of those laws . . . or otherwise significantly threatens or harms competition” under the tethering test. *Kellman*, 599 F. Supp. 3d at 896. Their allegation that Meta’s conduct “impaired competition within the market,” Compl. ¶ 436, is not only conclusory; it does nothing to tether their claim to a legislatively declared policy or proof of some actual or threatened impact on competition. *Kellman*, 599 F. Supp. 3d at 896.

CONCLUSION

The Court should dismiss the complaint with prejudice.

1 Dated: May 8, 2023

GIBSON, DUNN & CRUTCHER LLP

2 By: /s/ Lauren R. Goldman
Lauren R. Goldman

3 **COOLEY LLP**

4 By: /s/ Michael G. Rhodes
5 Michael G. Rhodes

6 *Attorneys for Meta Platforms, Inc.*
7 *(formerly known as Facebook, Inc.)*
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

CIVIL L.R. 5-1(h)(3) ATTESTATION

Pursuant to Civil Local Rule 5-1(h)(3), I, Lauren R. Goldman, hereby attest under penalty of perjury that concurrence in the filing of this document has been obtained from all signatories.

Dated: May 8, 2023

GIBSON, DUNN & CRUTCHER LLP

By: /s/ Lauren R. Goldman
Lauren R. Goldman

GIBSON, DUNN & CRUTCHER LLP
LAUREN R. GOLDMAN (*pro hac vice*)
lgoldman@gibsondunn.com
DARCY C. HARRIS (*pro hac vice*)
dharris@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) 393-4622
Facsimile: (415) 801-7389

ANDREW M. KASABIAN, SBN 313210
akasabian@gibsondunn.com
3161 Michelson Drive
Irvine, CA 92612 USA
Telephone: (949) 451-3800
Facsimile: (949) 451-4220

*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
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

IN RE META PIXEL HEALTHCARE
LITIGATION

This Document Relates To:

All Actions

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

**DEFENDANT META PLATFORMS, INC.'S
REQUEST FOR JUDICIAL NOTICE IN
SUPPORT OF ITS MOTION TO DISMISS**

CLASS ACTION

Date: August 16, 2023
Time: 2:00 p.m.
Courtroom 2

HON. WILLIAM H. ORRICK

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that pursuant to Federal Rule of Evidence 201(b), defendant Meta Platforms, Inc. (“Meta”), through its undersigned counsel, respectfully requests that the Court take judicial notice of, and/or deem as incorporated by reference, the following exhibits, filed in support of its Motion to Dismiss, which are attached to the accompanying Declaration of Abigail A. Barrera.

Exhibit 1 is a true and correct copy of Meta’s Terms of Service, available on Meta’s website: https://www.facebook.com/legal/terms/plain_text_terms.

Exhibit 2 is a true and correct copy of Meta’s Business Tools Terms, available on Meta’s website: <https://www.facebook.com/legal/terms/businessstools>.

Exhibit 3 is a true and correct copy of Meta’s Commercial Terms, available on Meta’s website: https://www.facebook.com/legal/commercial_terms.

Exhibit 4 is a true and correct copy of Meta’s Privacy Policy, available on Meta’s website: <https://mbasic.facebook.com/privacy/policy/printable/>.

Exhibit 5 is a true and correct copy of Meta’s Cookies Policy, available on Meta’s website: <https://mbasic.facebook.com/privacy/policies/cookies/printable/>.

Exhibit 6 is a true and correct copy of a webpage titled “Meta Pixel: Add a piece of code to your website that lets you measure, optimize and build audiences for your ad campaigns,” available on Meta’s website: <https://www.facebook.com/business/tools/meta-pixel>.

ARGUMENT

In ruling on a motion to dismiss, the Court may look beyond the four corners of the complaint to matters subject to judicial notice and documents incorporated in the complaint by reference. *See Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 998 (9th Cir. 2018); *Lee v. City of Los Angeles*, 250 F.3d 668, 688–89 (9th Cir. 2001). Meta respectfully requests that this Court take judicial notice of public records available on publicly available websites (Exhibits 1–6). Meta additionally requests the Court deem Exhibits 1–2 and 4–6 incorporated by reference because plaintiffs’ consolidated complaint depends on the contents of these documents.

A. Materials From Public Websites

The Court may take judicial notice of all six exhibits under Federal Rule of Evidence 201 because they are available on publicly available websites and the contents are not subject to reasonable dispute. *See* Fed. R. Evid. 201. Courts in this district routinely take judicial notice of websites and their contents, including publicly available contracts and terms of service. *See, e.g., Carvalho v. HP, Inc.*, 2022 WL 2290595, at *5 (N.D. Cal. June 24, 2022); *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1068–69 n.3 (N.D. Cal. 2016) (privacy policies); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1025 (N.D. Cal. 2014) (taking sua sponte judicial notice of privacy policies on publicly accessible websites); *Datel Holdings Ltd. v. Microsoft Corp.*, 712 F. Supp. 2d 974, 984 (N.D. Cal. 2010) (privacy policies); *see also Matthews v. Nat’l Football League Mgmt.*, 688 F.3d 1107, 1113 (9th Cir. 2012).

B. Material Incorporated By Reference

The Court may also take judicial notice of Exhibits 1, 2, 4, 5, and 6 under the incorporation by reference doctrine. Under the incorporation by reference doctrine, a district court may, when ruling on a motion to dismiss, consider documents outside the complaint when “the plaintiff’s claim depends on the contents of a document, the defendant attaches the document to its motion to dismiss, and the parties do not dispute the authenticity of the document, even though the plaintiff does not explicitly allege the contents of that document in the complaint.” *Knievel v. ESPN*, 393 F.3d 1068, 1076 (9th Cir. 2005); *accord Lee*, 250 F.3d at 688–89.

Exhibits 1, 2, 4, and 5—Meta’s Terms of Service, Business Tools Terms, Privacy Policy, and Cookies Policy—satisfy this standard. Plaintiffs refer selectively to these documents in their complaint. *See, e.g.,* Compl. ¶¶ 19, 86, 92–93, 96, 98–106, 114 & n.18, 121 & n.15. Exhibits 1, 4, and 5 also provide the basis for plaintiffs’ breach of contract claim. *See* Compl. ¶¶ 287–92, 300–02, 310, 312. Because these documents are “central to the plaintiff[s]’ claim[s]” and “no party questions the authenticity of the cop[ies] attached to” this Request, they are plainly subject to the incorporation-by-reference doctrine. *Marder v. Lopez*, 450 F.3d 445, 448 (9th Cir. 2006); *see, e.g., Varlack v. Ohio Sec. Ins.*, 2022 WL 17248997, at *1 (N.D. Cal. Nov. 28, 2022); *UAB “Planner 5D” v. Facebook, Inc.*, 2019 WL 6219223, at *2 n.2 (N.D. Cal. Nov. 21, 2019); *Letizia v. Facebook Inc.*, 267 F. Supp. 3d 1235, 1242 (N.D. Cal. 2017) (Facebook terms).

Exhibit 6—the article titled “Meta Pixel: Add a piece of code to your website that lets you measure, optimize and build audiences for your ad campaigns”—is also quoted and referenced repeatedly in the complaint. Compl ¶¶ 39, 41, 46 & nn.1, 3, 7. Further, this document—and what it does and does not say—“forms the basis” of plaintiffs’ claim that Meta violated plaintiffs’ rights because it explains how the Pixel works. *Khoja*, 899 F.3d at 1002; *see, e.g., Knievel*, 393 F.3d at 1076–77 (incorporating web pages related to specific representations cited in the complaint where the web pages were needed for context).

Consideration of these documents serves the core purpose of the incorporation by reference doctrine: to “preven[t] plaintiffs from selecting only portions of documents that support their claims, while omitting portions of those very documents that weaken—or doom—their claims.” *Khoja*, 899 F.3d at 1002; *see also Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1204 (N.D. Cal. 2014). The central theory of plaintiffs’ complaint is that Meta received their allegedly sensitive information without their consent. Meta’s policies form the basis of plaintiffs’ claims, and therefore the full text of these documents are essential for consideration of plaintiffs’ claims. Similarly, the “Meta Pixel: Add a piece of code to your website that lets you measure, optimize and build audiences for your ad campaigns” explains that third-party developers choose whether and how to install the Pixel on their websites. The full text of this article is therefore critical for the consideration of plaintiffs’ claims.

CONCLUSION

Under the incorporation by reference doctrine and Federal Rule of Evidence 201, and for the reasons stated above, the Court should consider Exhibits 1 through 6 to the accompanying Barrera Declaration when ruling on Meta’s motion to dismiss.

1 Dated: May 8, 2023

GIBSON, DUNN & CRUTCHER LLP

2 By: /s/ Lauren R. Goldman
3 Lauren R. Goldman

COOLEY LLP

4 By: /s/ Michael G. Rhodes
5 Michael G. Rhodes

6 *Attorneys for Meta Platforms, Inc.*

CIVIL L.R. 5-1(h)(3) ATTESTATION

Pursuant to Civil Local Rule 5-1(h)(3), I, Lauren R. Goldman, hereby attest under penalty of perjury that concurrence in the filing of this document has been obtained from all signatories.

Dated: May 8, 2023

GIBSON, DUNN & CRUTCHER LLP

By: /s/ Lauren R. Goldman
Lauren R. Goldman

GIBSON, DUNN & CRUTCHER LLP
LAUREN R. GOLDMAN (*pro hac vice*)
lgoldman@gibsondunn.com
DARCY C. HARRIS (*pro hac vice*)
dharris@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) 393-4622
Facsimile: (415) 801-7389

ANDREW M. KASABIAN, SBN 313210
akasabian@gibsondunn.com
3161 Michelson Drive
Irvine, CA 92612 USA
Telephone: (949) 451-3800
Facsimile: (949) 451-4220

*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
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

IN RE META PIXEL HEALTHCARE
LITIGATION

This Document Relates To:

All Actions

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

**DECLARATION OF ABIGAIL A. BARRERA
IN SUPPORT OF DEFENDANT META
PLATFORMS, INC.'S MOTION TO
DISMISS THE CONSOLIDATED CLASS
ACTION COMPLAINT**

CLASS ACTION

Date: August 16, 2023
Time: 2:00 p.m.
Courtroom 2

HON. 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 at
3 the law firm of Gibson, Dunn & Crutcher LLP, and I represent Meta Platforms, Inc. (“Meta”) in the
4 above-referenced action. I submit this declaration in support of Meta’s Motion to Dismiss the
5 Complaint. Unless otherwise stated, the following facts are within my personal knowledge and, if
6 called and sworn as a witness, I could and would testify competently to them.

7 2. Attached hereto as **Exhibit 1** is a true and correct copy of Meta’s Terms of Service dated
8 July 26, 2022, downloaded from Meta’s website at
9 https://www.facebook.com/legal/terms/plain_text_terms.

10 3. Attached hereto as **Exhibit 2** is a true and correct copy of Meta’s Business Tools Terms
11 dated August 31, 2020, downloaded from Meta’s website at
12 <https://www.facebook.com/legal/terms/business tools>.

13 4. Attached hereto as **Exhibit 3** is a true and correct copy of Meta’s Commercial Terms
14 dated January 4, 2022, downloaded from Meta’s website at
15 https://www.facebook.com/legal/commercial_terms.

16 5. Attached hereto as **Exhibit 4** is a true and correct copy of Meta’s Privacy Policy dated
17 January 1, 2023, downloaded from Meta’s website at
18 <https://mbasic.facebook.com/privacy/policy/printable/>.

19 6. Attached hereto as **Exhibit 5** is a true and correct copy of Meta’s Cookies Policy dated
20 October 5, 2022, downloaded from Meta’s website at
21 <https://mbasic.facebook.com/privacy/policies/cookies/printable/>.

22 7. Attached hereto as **Exhibit 6** is a true and correct copy of a webpage titled “Meta Pixel:
23 Add a piece of code to your website that lets you measure, optimize and build audiences for your ad
24 campaigns,” downloaded from Meta’s website at [https://www.facebook.com/business/tools/meta-](https://www.facebook.com/business/tools/meta-pixel)
25 [pixel](https://www.facebook.com/business/tools/meta-pixel).

Executed this 8th day of May, 2023 in San Francisco, California.



Abigail A. Barrera

Exhibit 1

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.

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 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.

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](#).

3. Your commitments to Facebook 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:

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.

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):

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.

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.

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.

You may not proxy, request, or collect Product usernames or passwords, or misappropriate access tokens.

You may not sell, license, or purchase any data obtained from us or our services, except as provided in the Platform Terms.

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.

The permissions you give us

We need certain permissions from you to provide our services:

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.

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.

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.

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](#).

4. Additional provisions

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 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.

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.

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, 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.

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.

Other

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.

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.

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.

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

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.

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.

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).

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.

We reserve all rights not expressly granted to you.

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](#)



[Privacy](#) · [Terms](#) · [Advertising](#) · [Ad Choices](#)  · [Cookies](#) · [More](#) · Meta © 2023

Exhibit 2

[Log In](#)

We're updating our Business Tools Terms. The updates go into effect on 25 April 2023. See new terms [here](#).

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

Case 3:22-cv-03580-WHO Document 232-4 Filed 05/08/23 Page 3 of 7

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. Note to Korean advertisers: To the extent the Business Tool Data contain Personal Information which you process subject to applicable laws, you must ensure that an end user provides the necessary consent under applicable laws as required under Section 1.e. for Facebook's use of the Business Tool Data for the benefit of Facebook as described in Section 2.a.v. Please refer to Facebook's **Data Policy** for further information about Facebook's processing of Personal Information.
- 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

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

[Sign Up](#) [Log In](#) [Messenger](#) [Facebook Lite](#) [Watch](#) [Places](#) [Games](#) [Marketplace](#) [Meta Pay](#) [Meta Store](#) [Meta Quest](#)

[Instagram](#) [Bulletin](#) [Fundraisers](#) [Services](#) [Voting Information Center](#) [Privacy Policy](#) [Privacy Center](#) [Groups](#)

[Privacy](#) · [Terms](#) · [Advertising](#) · [Ad Choices](#)  · [Cookies](#) · [More](#) · Meta © 2023

Exhibit 3


[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.

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.

1. **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.
2. **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.
3. **Data Restrictions:** You may not send us information prohibited by the supplemental terms or

Case 3:22-cv-03580-WHO Document 232-5 Filed 05/08/23 Page 3 of 7

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.

4. **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.

5. **Disputes:**

- a. **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.
- b. **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.
- c. **U.S. Commercial Claims:** If you reside in the United States or your business is located in the United States:
- i. 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.

- ii. 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.

- d. 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:

- i. 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.

- ii. 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.
- iii. 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.
- iv. 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.

e. 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.

6. 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.

7. 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.

a. 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.

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

- c. Except as permitted in Section 6, any amendment to or waiver of these Commercial Terms must be made in writing and signed by us.
- d. You will not transfer any of your rights or obligations under these Commercial Terms to anyone else without our consent.
- e. These Commercial Terms do not confer any third party beneficiary rights.
- f. 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.
- g. 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.
- h. 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.
- i. 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.
- j. Nothing in these Commercial Terms or any applicable supplemental terms will prevent us from complying with the law.
- k. 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) 中文(简体) 日本語 한국어 Français (France) Bahasa Indonesia Polski Español Português (Brasil) Deutsch Italiano

[Sign Up](#) [Log In](#) [Messenger](#) [Facebook Lite](#) [Watch](#) [Places](#) [Games](#) [Marketplace](#) [Meta Pay](#) [Meta Store](#) [Meta Quest](#)
[Instagram](#) [Bulletin](#) [Fundraisers](#) [Services](#) [Voting Information Center](#) [Privacy Policy](#) [Privacy Center](#) [Groups](#)

Exhibit 4



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 United States residents



How to contact Meta with questions





Other policies

Terms of Service



Cookies Policy



What is the Privacy Policy and what does it cover?

Effective January 1, 2023

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](#), such as Meta Horizon Worlds or Meta Quest (when using a Facebook or Meta 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



Meta Platforms Technologies Products



Oversight Board



[Return to top](#) ^

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

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

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.

7

Metadata about content or messages

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.

Return to top ^

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 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 use [information with special protections](#) you choose to provide for these purposes, but not 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.

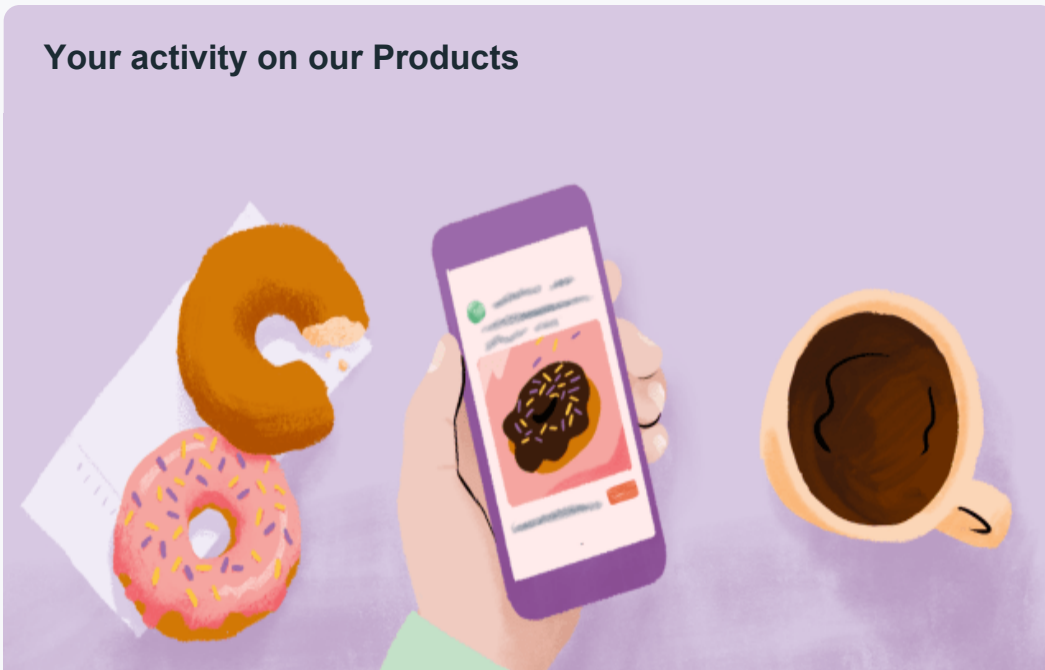
More resources

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.

27

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.

Return to top ^

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 business 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:

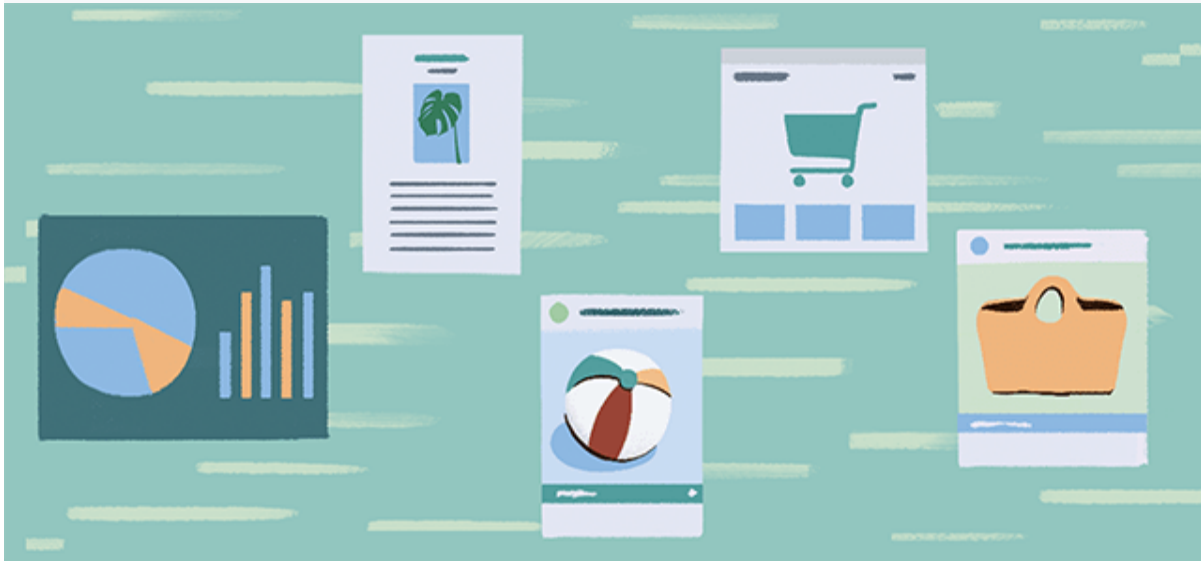
- They can view and access a list of your Facebook friends who use the same app and have given the app permission to access their list of friends. They can't access nonpublic information about your friends or followers through this process. Note that the app developer will receive more information about 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

[Return to top](#) ^

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.

39

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

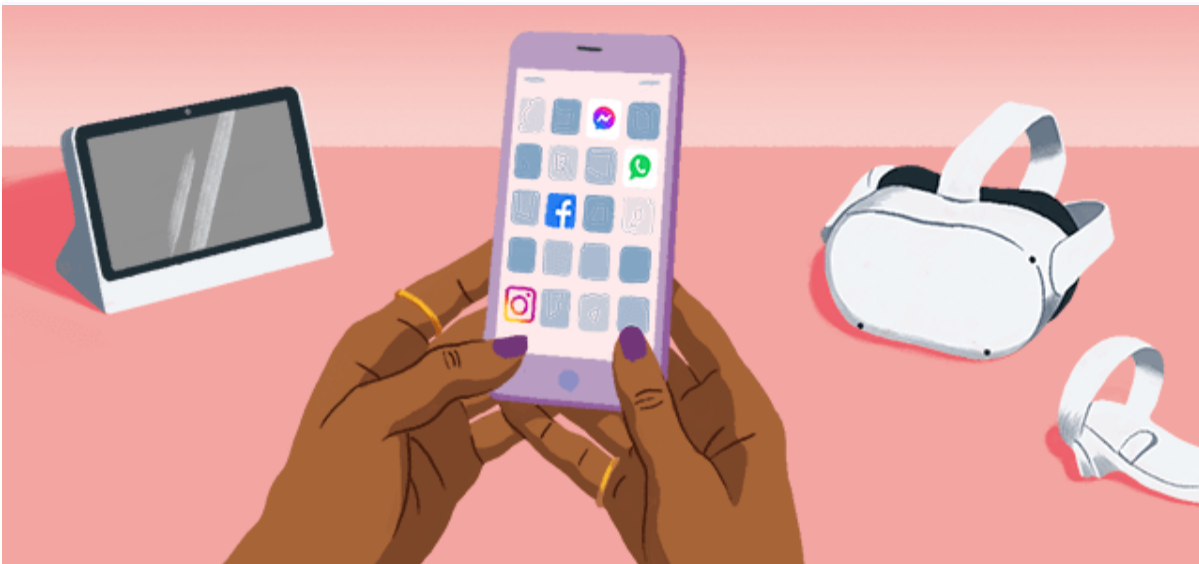
For example, vendors:

- 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.

[Return to top](#) ^

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 [Facebook Help Center](#)



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.

46

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.

Return to top ^

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 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.

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.

Return to top ^

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.

[Return to top](#) ^

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.

Return to top ^

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.

[Return to top](#) ^

Privacy notice for United States residents

You can learn more about the consumer privacy rights that may be available to you by reviewing the [United States Regional Privacy Notice](#).

[Return to top](#) ^

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

[Return to top](#) ^

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</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

personalized experiences across the Meta Products in accordance with our terms. This is how we:

- 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.

[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.

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

[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 (like GPS location)
- Information about the network you connect your device to
- Reports about our products'

	<p>performance on your device</p> <ul style="list-style-type: none"> • 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 • 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 	<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 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>products or features, and</p> <ul style="list-style-type: none"> • Conduct surveys and other research about what you like about our Products and brands and what we can do better. 	<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>
<p>Promoting safety, integrity and security 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:</p> <ul style="list-style-type: none"> • Verify accounts and activity, • Find and address violations of our terms or policies. In some cases, the 	<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

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](#).

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'
- 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
<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 • 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.
Transferring, storing or processing your information across borders, including from and to the United States and other	Your activity and information you provide:

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:

- 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.

For more information, see the "[How do we transfer information?](#)" section of the Meta Privacy Policy.

- 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

[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 advice apart from other users'
- Device signals
- Information you've shared

	<p>through your device settings</p> <ul style="list-style-type: none"> • 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>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>	<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
<p>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 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>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>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>	<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

<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>comments</p>
<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 content and ads are performing on and off Meta Products, and • 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. 	<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 • 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 • 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

	<ul style="list-style-type: none"> • 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>Business intelligence and analytics:</p> <ul style="list-style-type: none"> • 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. 	<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

	<p>interact with, and how you interact 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 • 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>
Identifying you as a Meta Product user	Your activity and information you

and personalizing the ads we show you through Meta Audience Network when you visit other apps:

- 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.

provide:

- 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

[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

	<p>through your device settings</p> <ul style="list-style-type: none"> • 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. • 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 	<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

create COVID-19 forecasting models.

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

- 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
- Information from cookies and similar technologies

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

Anonymizing your information

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.

[Your activity and 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

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
- Information from cookies and similar technologies

Information from Partners,

	vendors and third parties
<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 • 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 <p>Learn more about how we promote safety, security and integrity.</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, 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> <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

	<p>through your device settings</p> <ul style="list-style-type: none"> • 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>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.</p> <p>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 operational guidelines law enforcement needs to follow.</p>	<p>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:</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 • 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'
- 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](#)

Exhibit 5



Cookies Policy

Explore the policy

What are cookies, and what does this policy cover?



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?



Other policies

Terms of Service



Cookies Policy



What are cookies, and what does this policy cover?

Effective October 5, 2022

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 [Privacy 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 `_fbp` 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^{\[1\]}](#) 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.

1

List of Companies

Listed below are the names and websites of some of the companies that use cookies on the Facebook Services to provide services to us and the businesses that advertise on Facebook.

Last update: September 13, 2021

Company	Website
A9	https://www.a9.com
Ada	https://www.ada.support
Adclear	https://www.adclear.de
Adform	https://site.adform.com
AdGear	https://www.adgear.com

Addition	https://www.addition.com
Adobe	https://www.mktorep.com
Adobe Business Catalyst	https://www.businesscatalyst.com
Adometry	https://www.adometry.com/tv-attribution
AdParlor	https://www.adparlor.com
Adslot	https://www.adslot.com
Akamai	https://akamaihd.net
Amazon Web Services	https://www.cloudfront.net
Ancestry	https://www.ancestry.com
Autodesk	https://www.autodesk.com
Clarabridge	https://www.engagor.com
comScore	https://www.comscore.com
Conversant Media	https://www.conversantmedia.com

Convertro	https://www.convertro.com
DA Consortium	https://www.dac.co.jp
Datalicious	https://www.datalicious.com
DoubleClick	https://www.doubleclickbygoogle.com
Eyeturn Marketing	https://www.eyeturnmarketing.com
Flashtalking	https://www.flashtalking.com
GfK	https://www.gfk.com
Giphy	https://www.giphy.com
Google	https://www.google.com/
Google	https://www.doubleclick.net/
Google	https://www.google-analytics.com
Google	https://www.googleadservices.com

Google	https://www.googleapis.com
Google	https://www.googletagmanager.com
Google	https://www.gstatic.com
Google	https://www.youtube.com
Google	https://www.ytimg.com
Hive Streaming	https://www.hivestreaming.com
Integral Ad Science	https://www.integralads.com/
Intuit	https://www.intuit.com
Ipsos	https://www.ipsos.com
Jio	https://www.jio.com
Kantar World Panel	https://www.kantarworldpanel.com
Kenshoo	https://kenshoo.com
Linkedin	https://www.linkedin.com

Linkedin	https://www.adsymptotic.com
Linkedin	https://www.licdn.com
Mapbox	https://www.mapbox.com
Markit	https://www.markit.com
Maxar	https://www.digitalglobe.com
Meetrics	https://www.meetrics.com
Megaphone	https://www.megaphone.fm/
Metrix Lab	https://www.metrixlab.com
Microsoft	https://www.bing.com
Microsoft	https://www.virtualearth.net
Millward Brown	https://www.millwardbrowndigital.com
Mixpanel	https://www.mixpanel.com
Moat	https://moat.com/

Nanigans	https://www.nanigans.com
Neustar	https://www.neustar.biz
Next Audience	https://next-audience.com
Nielsen	https://www.nielsen.com
Paypal	https://www.paypal.com
Podsights	https://www.pdst.fm
Podtrac	https://analytics.podtrac.com/
Rakuten	https://marketing.rakuten.com
Reddit	https://www.redditstatic.com
Reddit	https://www.reddit.com
Research Now	https://www.researchnow.com
Salesforce	https://www.herokuapp.com

Sapient	https://publicis.sapient.com
Shift	https://www.shiftcomm.com
Shopify	https://www.shopify.com
Sizmek	https://www.sizmek.com
Smart Adserver	https://smartadserver.com
Spreaker	https://www.spreaker.com/
Stackla	https://www.stackla.com
Symphony Advanced Media	https://www.symphonym.com
Tealium	https://www.tiqcdn.com
Tenor	https://www.tenor.co
Tenor	https://www.tenor.com
The Trade Desk	https://www.thetradedesk.com/
The Trade Desk	https://www.adsrvr.org

ThreatMetrix	https://www.threatmetrix.com/
Trend Research	https://www.trendresearch.com
Twitter	https://twitter.com/
Twitter	https://www.ads-twitter.com
Twitter	https://www.twimg.com
Twitter	https://t.co
UserReport	https://www.userreport.com
Visa	https://www.cardinalcommerce.com
Visual IQ	https://www.visualiq.com
Weborama	https://www.weborama.com
White Ops	https://www.whiteops.com/
Xaxis	https://www.xaxis.com

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](#)

Return to top ^

Exhibit 6

Meta Pixel

Add a piece of code to your website that lets you measure, optimize and build audiences for your ad campaigns.



✓ Introduction

What is the Meta Pixel?

The Meta Pixel is a piece of code on your website that can help you better understand the effectiveness of your advertising and the actions people take on your site, like visiting a page or adding an item to their cart. You'll also be able to see when customers took an action after seeing your ad on Facebook and Instagram, which can help you with retargeting. And when you use the Conversions API alongside the Pixel, it creates a more reliable connection that helps the delivery system decrease your costs.



Get Started



⌵ Key Features

Optimize the delivery of your ads.

Ensure your ads reach the people most likely to take action.

Measure cross-device

Understand how your cross-device a

Personalized Plan

Get marketing guidance tailored to your goals.

Find tips, resources and tools to track progress towards your goals with a personalized marketing plan.

[Go to My Plan](#)

Was this page helpful?

☒ Yes ☐ No

Meta Technologies



Guides and Resources



Business Help Center



© 2023 Meta



[About](#) [Developers](#) [Careers](#) [Privacy](#) [Cookies](#) [Terms](#) [Help Center](#)

[English \(US\)](#) [English \(UK\)](#) [Español](#) [Português \(Brasil\)](#) [Français \(France\)](#) [Español \(España\)](#) [More languages >](#)

GIBSON, DUNN & CRUTCHER LLP
LAUREN R. GOLDMAN (*pro hac vice*)
lgoldman@gibsondunn.com
DARCY C. HARRIS (*pro hac vice*)
dharris@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) 393-4622
Facsimile: (415) 801-7389

ANDREW M. KASABIAN, SBN 313210
akasabian@gibsondunn.com
3161 Michelson Drive
Irvine, CA 92612 USA
Telephone: (949) 451-3800
Facsimile: (949) 451-4220

*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
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

IN RE META PIXEL HEALTHCARE
LITIGATION

This Document Relates To:

All Actions

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

**[PROPOSED] ORDER GRANTING
DEFENDANT META PLATFORMS, INC.'S
MOTION TO DISMISS THE COMPLAINT**

CLASS ACTION

1 On May 8, 2023, defendant Meta Platforms, Inc. filed a Motion to Dismiss the Complaint. The
2 Court, having fully reviewed and considered all papers and arguments submitted in support of and in
3 opposition to the Motion, and finding good cause for the Motion, orders as follows:

4 **IT IS HEREBY ORDERED** that Meta's Motion to Dismiss is **GRANTED**. All claims and
5 causes of actions are hereby **DISMISSED WITH PREJUDICE**.

6
7
8 Dated: _____
9

10 _____
11 HON. WILLIAM ORRICK
12 United States District Court Judge
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28