ROB BONTA
Attorney General of California
NICKLAS A. AKERS
Senior Assistant Attorney General
STACEY D. SCHESSER
Supervising Deputy Attorney General
MICAH C.E. OSGOOD (SBN 255239)
MANEESH SHARMA (SBN 280084)
ANDREW J. WIENER (SBN 282414)
CAROLINE E. WILSON (SBN 322389)
Deputy Attorneys General
455 Golden Gate Ave. Suite 11000
San Francisco, CA 94102
Telephone: (415) 510-3500
mike.osgood@doj.ca.gov
Attorneys for People of the State of California

[EXEMPT FROM FILING FEES GOVERNMENT CODE § 6103]

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF SAN FRANCISCO

PEOPLE OF THE STATE OF CALIFORNIA, Plaintiff, **v.** **META PLATFORMS, INC.,** Defendant.	Case No. **CGC-25-631678** **COMPLAINT FOR INJUNCTION, CIVIL PENALTIES, AND OTHER EQUITABLE RELIEF** (BUS. & PROF. CODE, §§ 17206 & 17500)

The People of the State of California, through Attorney General Rob Bonta, bring this action against Meta Platforms, Inc. ("Meta") for violations of California's consumer protection laws. The People allege the following facts based on information and belief:

INTRODUCTION

1. For years, Meta deceived consumers regarding their ability to limit the audience of the personal details they uploaded to Facebook. Users believed they could limit their information to their Facebook "Friends" using various privacy settings. But in reality, Meta granted millions of third-party apps access to that same "Friend Data" through the Facebook "App Platform." The most infamous of these apps, "This Is Your Digital Life" and its developer Aleksandr Kogan,

collected and sold Friend Data to Cambridge Analytica in 2013. This affected an estimated seven million California Facebook users. Meta likely could have prevented this sale and the ensuing scandal, had senior leaders not ignored multiple red flags that apps improperly accessed Friend Data over the years. Meta's deceptive privacy settings and failure to enforce its own policies or remove apps' access to Friend Data violated California law in multiple ways.

2. First, Meta unlawfully deceived users by prominently telling them they could limit access to their personal details to their Friends, while downplaying how third-party apps had broad access to that same data. This was despite external reports and internal research showing that users didn't understand the App Platform and thought limiting data to "Friends" meant just that. What's more, by late 2012, Meta had made it more difficult for users to control access to their data, by removing all references to apps from Facebook's privacy settings page and burying the specific privacy settings for Apps elsewhere in the user interface. Meta also allowed secret "whitelisted" apps to override these buried app privacy settings entirely.

3. Second, Meta deceived users by claiming to aggressively enforce its App Platform policy against apps for improperly accessing Friend Data. Records show Meta almost never enforced this policy, despite the company's estimates that hundreds of thousands of apps violated this policy. Executives fretted that enforcement might cause app developers to abandon the App Platform while the company sought to turn the platform into a money-making enterprise.

4. Third, Meta's deceptive conduct described above violated its 2012 consent order with the Federal Trade Commission, which is actionable under California law as a per se unlawful business practice. The FTC had required that Meta not override users' limitations on their chosen audiences for their data, without a clear and conspicuous disclosure to that effect. Meta also violated the FTC order by not maintaining a "comprehensive privacy program" to adequately assess ***and mitigate*** the risk of any unauthorized sharing of users' data with third parties, such as by enforcing policies meant to protect users.

5. Meta's senior leaders knew of and often participated in the decisions that led to the conduct that violated California law. As far back as 2012, senior leaders acknowledged that "we leak info to developers" through the App Platform. Nevertheless, they approved changes to the

privacy settings pages that buried mention of how users could limit apps' access to Friend Data. Senior leaders also dismissed the need for greater app policy enforcement, noting that the focus should be "clearly defining what we want and don't want, rather than catching apps [doing] sketchy things. It's not that the latter isn't a problem. . . ." And in late 2012, when other senior leaders pressed CEO Mark Zuckerberg to cut off apps' access to Friend Data, he refused for years, possibly to protect Meta's then-foundering stock price.

6. This case reinforces two obligations with which businesses must comply. First, businesses cannot deceive consumers when describing how they use and disclose data to third parties, including in the user interface's privacy settings and related descriptions. Nor can businesses claim that a rarely read privacy policy or buried privacy setting somehow cures more prominent, but deceptive, statements in the portions of the user interface with which consumers regularly interact. Second, businesses must also comply with federal consent orders regarding users' privacy. A violation of such an order is actionable under California's Unfair Competition Law as an unlawful business practice. Meta didn't comply with either of these obligations and so its disclosure of Friend Data to third-party app developers violated California's Unfair Competition and False Advertising laws.

THE PARTIES

7. Plaintiff is the People of the State of California. The People bring this action through Attorney General Rob Bonta, who has authority to bring this suit under the Unfair Competition and False Advertising Laws. (See Bus. & Prof. Code §§ 17204, 17206, 17535, & 17536.)

8. Defendant Meta, originally doing business as Facebook, Inc., is a Delaware corporation, headquartered in Menlo Park, California. Meta has employees and maintains office space in San Francisco, California.

JURISDICTION AND VENUE

9. Meta has and continues to conduct business within the State of California, including the City and County of San Francisco. The violations of law described herein were committed in the City and County of San Francisco and elsewhere in the State of California.

DEFENDANT'S BUSINESS ACTS AND PRACTICES

I. THE FACEBOOK SERVICE AND APP PLATFORM.

10. Among other endeavors, Meta operates the Facebook social media service that allows individuals to create personalized profiles, filled with biographical details, photos, and "posts" by the user. Users can post and share personal details like their date of birth, hometown, employer, relationship status, spouse's name, political views, sexual orientation, photos of children, and membership in various groups. Facebook also lets users connect with other users as "Friends," and as relevant here, purported to allow users to restrict who can access their information using various privacy settings. Meta estimates that from 2014 to 2020, over 20 million Californians used the Facebook service at least once every month.

11. In 2007, Meta launched the Facebook App Platform, which let third-party developers create applications for Facebook users. Facebook apps included popular games and personality quizzes. Meta granted third-party developers access to data about users, ostensibly to allow for personalization. For example, a horoscope app might access a user's birthdate to provide the correct horoscope. But as Meta knew years before taking any action to stop it, apps abused this access to capture user information unrelated to the app's function. At its peak, the App Platform had millions of apps.

II. META AND ITS SENIOR EXECUTIVES KNEW OF THE RISKS POSED BY THE APP PLATFORM AND APPS' ACCESS TO FRIEND DATA.

12. Senior leaders, including Zuckerberg, knew of the risks posed by apps accessing Friend Data long before Kogan's "This is Your Digital Life" app began collecting and selling Friend Data to Cambridge Analytica. One former senior executive testified that a debate over privacy and apps' access to data began "before [Facebook] even launched the first version [of the App Platform]" in 2007.

13. In 2011, in prelude to its first settlement with Meta, the FTC alleged that the company misled users about the App Platform. Specifically, the FTC alleged that Meta had told users they could limit data to Friends, when such data also went to apps. The FTC also alleged that apps sought access to data they did not need. These allegations led to the 2012 FTC consent order.

14. In April of 2012, the Wall Street Journal published an article sounding the alarm about apps' access to Friend Data. The Journal noted that apps still asked for Friend Data that was not used in the app, including sensitive information such as "the sexual preferences of users and their friends." The article noted that this violated Meta's App Platform policies. Meta responded, publicly stating that when it "find[s] an app has violated our policies . . . we take action." Over the next eight months, senior leaders discussed the problems with the App Platform. This included discussing that "tons" of apps potentially violated App Platform policies by acquiring Friend Data. Senior leaders raised to the highest level that "[n]o developers" used Friend Data "for anything good," prompting Zuckerberg to say he was "open to closing this down." Later, he testified that "some of [these apps] were just downright abusive."

15. By the fall of 2012, multiple senior leaders were pleading with Zuckerberg to cut off apps' access to Friend Data. Zuckerberg appears to have initially relented, agreeing that apps would lose access to Friend Data. But by early 2013, Zuckerberg reversed course, placing the change on indefinite hold. Had Meta acted, as initially agreed in late 2012, Kogan may not have acquired the data he later sold to Cambridge Analytica. Ultimately, Meta did not cut off access to Friend Data until April of 2014 for new apps and until April 2015 for most existing apps.

16. Meta may have delayed removing apps' access to Friend Data for financial reasons. In 2012, Meta had gone public, and its stock price fell due to declining ad revenue. While internally discussing the need to remove apps' access to Friend Data, Meta publicly detailed plans to monetize the App Platform in a variety of potential ways. Zuckerberg emailed senior leaders about the need to generate more revenue, including finding new ways to make money from existing products. And in one email regarding the proposal to cut off apps' access to Friend Data, he explicitly cautioned that "I'm not sure how far we'll get without figuring out monetization as well." Ultimately, the App Platform changed only after the stock price recovered.

III. FACEBOOK'S DECEPTIVE USER INTERFACE CONCEALED DISCLOSURE OF USERS' DATA TO APPS.

17. Meta's pattern of placing profits over users' privacy continued when it updated Facebook's privacy settings in 2012. There, the user interface deceived users through false or

misleading statements and by burying key settings in places few users would find.

A. Overview of Facebook's privacy control scheme.

18. While the precise layout and wording changed over time, Facebook's privacy control scheme generally stayed the same. Meta told users that they could limit Facebook posts and personal details to certain "audiences." For example, users could limit whether their religion, birthdate, birth year, and the like, would be seen by "Everyone," "Friends," or "Only Me." Meta refers to this type of privacy setting as an "audience selector."

19. But the audience selectors did not prevent information from going to an app installed by the user's Friends. In other words, selecting the "Friends" audience did not mean just Friends, it also meant Friends' apps and the apps' developers. Thus, the word "Friends" in the audience selector was deceptive. To prevent apps from accessing Friend Data, a user had to find and use a ***separate*** App Platform privacy setting, which Meta buried and knew most users wouldn't find.

B. The December 2012 changes to Facebook privacy settings and subsequent updates further concealed that user data was being shared with apps.

20. In December 2012, Meta changed Facebook's primary privacy settings page, removing all references to apps and the specific privacy setting that prevented an app from accessing Friend Data. The "Privacy Settings and Tools" page instead offered users "Who can see my stuff?" and "Who can look me up?" even though neither prompt lead to any settings relating to apps that could "see" and "look up" Friend Data. Instead, those prompts explained how other Facebook users could access certain data. Meta's prior version of this page expressly mentioned apps and linked to the privacy setting for Friend Data. Meta also created "Privacy Shortcuts," which was a small popup with similar prompts. Like the Privacy Settings and Tools page, Privacy Shortcuts made no mention of apps' access to Friend Data or the privacy setting for Friend Data.

21. Meta also deceived users about apps' access to information under Facebook's newly created "Apps Settings" page. There, Meta told users that both people and apps had access to certain information that was "always publicly available," like the user's name, and that apps had "access to your friends list and any information you choose to make public." On the same App Settings page near the bottom, Meta buried the setting that actually prevented a user's personal

information from going to apps installed by a Friend in a link under "Apps Others Use." This link was hard to find because Meta placed the notification in a subdued font and in the lower corner of a screen that had dozens of clickable elements. Company documents conceded that only a "power user" would find this app-specific privacy setting. And under the link, Meta deceptively stated that a users' Friends had to "bring" Friend Data with them to an app, rather than explaining that a Friend's mere installation of an app granted immediate and continual access to Friend Data.

22. Meta continued to avoid telling users that apps could access information about them through their friends. Beginning in 2014, Meta invited users for a "Privacy Checkup" that was supposed to allow users "to review and control who [they're] sharing with." The Privacy Checkup mentioned apps, but only to remind users of the option to limit who "sees each app you use and any future posts it makes for you." Again, Meta failed to mention apps' getting access to data or the separate app privacy settings. Senior leaders, including Zuckerberg, testified that they likely approved these settings, including the 2012 removal of apps from the privacy settings page.

C. Meta knew Facebook's privacy user interface confused and misled users.

23. Meta knew for years that Facebook privacy settings confused users. In 2010, Meta acknowledged that users wanted a "simpler way" to control their data, promising to "add privacy controls that are much simpler to use." Meta also maintained a chart summarizing academic research, including studies showing that "Facebook users' privacy settings don't match their intentions." The chart also included detailed notes on academic papers arguing that Facebook has "privacy choices that are illusory opt-outs and sleight-of-hand 'messaging.'"

24. Meta also knew that its audience selector model, specifically, misled users. Internal 2012 research confirmed that "[u]sers expected the [audience selector] to be the universal truth[,]" and that once users changed the audience selector to "Friends," it would "take care of everything[.]" In 2014, when Meta finally announced that apps would lose access to Friend Data, Zuckerberg's keynote address justified the change because users were "surprised when one of [their] friends shares some of [their] data with an app," which was "not good for anyone."

25. Meta's misleading disclosures described above not only deceived users, but they also violated the FTC's 2012 consent order. There, the FTC ordered Meta to "clearly and

prominently" disclose certain information before sharing a user's information with any third party, when such sharing would materially differ from the user's privacy settings. This included sharing Friend Data beyond the user's Friends. But Meta did not conspicuously disclose apps' access to Friend Data. Instead, Meta removed or buried references to apps' access to Friend Data.

IV. META CONCEALED THAT "WHITELISTED" APPS RECEIVED SPECIAL ACCESS TO USERS' PERSONAL INFORMATION.

26. Meta also deceived Facebook users by granting certain "capabilities" to a privileged subset of apps to access a user's and their Friends' data even when the user's app privacy settings would otherwise have blocked such access. Meta referred to this practice as "whitelisting," and thousands of whitelisted apps had access to Facebook's systems in ways other apps did not. As one example of such a capability, Facebook granted certain apps access to a user's ***and their Friends'*** "likes, location, education, work, status, presence, relationship status, wall, notes, groups, events, photos, religion, looking for, significant other, website, activities, [and] interests."

27. The amount of user data made available to privileged apps through whitelisting was significant. One senior Meta employee described the amount of data available to whitelisted apps as "crazy." That same employee found in 2013 that 3700 whitelisted apps had a negligible number of active users, yet frequently accessed Friend Data.

28. Even after making its 2014 announcement that apps would lose access to Friend Data, Meta allowed some whitelisted apps to continue accessing Friend Data. What's more, Meta never gave people any ability to opt out of this disclosure of their personal information. The (buried) App Platform privacy setting had no effect on Friend Data going to certain whitelisted apps.

29. Like with the regular apps, Meta's sharing of user data with whitelisted apps was deceptive and violated the FTC's 2012 order, by sharing Friend Data beyond the users' Friends.

V. META FALSELY TOLD THE PUBLIC THAT IT ENFORCED ITS POLICIES TO PROTECT USERS, BUT WHOLLY FAILED TO ENFORCE POLICIES AROUND FRIEND DATA.

30. Meta consistently told the public that it took aggressive action to enforce its policies and protect users. But that simply wasn't true. Between 2010 and 2016, Meta made at least seven false public statements describing the robustness of its policy enforcement efforts. Meta told the

Wall Street Journal of its "strong policy enforcement" on one occasion. Later, Meta told the Journal that "[i]f we find an app has violated our policies . . . we take action." Another time, Meta told a journalist that it takes "strong measures to enforce" an app-related policy "including suspending and disabling applications that violate it." Later, Meta described its "vigilan[ce]" in "protecting our users from those who would try to expose any form of user information . . . we take aggressive action on reports just like these." On three other occasions, when asked about allegations of apps' misbehavior by various media outlets, Meta claimed to "act swiftly" or "take swift action" when apps violated App Platform policies.

31. Meta knew that each of these statements was false or materially misleading because Meta knew apps improperly accessed data and that it didn't enforce its policies. Multiple internal documents discuss both specific apps and problems with the App Platform more generally. For example, one Meta presentation from mid-2012 detailed "the abuse" Meta had observed on the App Platform, including apps asking for Friend Data the app didn't need in violation of App Platform policies. This presentation was created by employees that enforced the App Platform policies. These employees also created a chart of allegations raised by the 2012 Wall Street Journal article about apps and the company's responses. One of those allegations was that "Apps [were] asking for more data than they need to operate." These employees also appeared to have met with a senior leader to discuss a series of remediation efforts that never happened. Senior leaders also discussed apps improperly accessing Friend Data in 2012, in their deliberations over whether apps' should lose access to Friend Data and the need to enforce App Platform policies.

32. Meta did at least look further into the issues with apps, but it still took no action. In a March 2013 audit of hundreds of apps, Meta found that 40 percent committed at least one App Platform policy violation. Another audit showed that 10 percent of all apps violated the policy against accessing unnecessary Friend Data, including "high risk" data. Meta employees also discussed that numerous apps accessed users' information through the App Platform in a manner that was far out of proportion to the number of people using an app, an obvious red flag.

33. But Meta did nothing with these findings. Despite estimating that hundreds of thousands of apps on the App Platform requested unnecessary Friend Data, Meta could only

identify 63 instances between 2012 and 2018 where it took action for violating ***any*** of Meta's policies relating to data misuse. Meta's most comprehensive database of app policy violations revealed only ***a single enforcement*** action against an app accessing Friend Data during the 2012 or 2013 period, despite the public reports and Meta's audits finding rampant policy violations.

34. Meta's false statements about enforcing policies when it found violations broke California law and ran afoul of the FTC order's requirement that Meta act to protect users' data.

VI. META FAILED TO ASSESS AND MITIGATE RISKS OF THE APP PLATFORM, DESPITE THE FTC ORDER MANDATING THAT THE COMPANY DO SO.

35. In the 2012 consent order, the FTC mandated that Meta create a "comprehensive privacy program." As part of that privacy program, Meta was tasked with identifying "reasonably foreseeable, material risks" that "could result" in Meta collecting, using, ***or disclosing*** users' information without their permission. The order then required Meta to "address the risks identified through the privacy risk assessment," and to conduct "regular testing or monitoring of the effectiveness" of the mitigation measures Meta employed to address those risks. And as noted above, this order arose from allegations of apps' access to Friend Data. Meta told the FTC that to meet its obligations, Meta would run new products or changes to products by a specialty privacy committee, conduct formal Privacy Risk Assessments, and hold annual privacy summits to review the Privacy Risk Assessment. Meta fell far short in complying with these measures.

36. First, Meta failed to assess and mitigate privacy risks when it launched or altered products. For example, Meta could not produce records showing that it assessed the privacy risks of the 2012 privacy settings changes, which removed all mentions of apps. Nor was there any evidence that Meta assessed the privacy risks when it whitelisted new apps.

37. Second, Meta's assessments of risks posed by existing products—like the App Platform—was deeply flawed. For example, Meta's 2013 Privacy Risk Assessment identified the risk that users may fail "to use the controls offered to limit others from sharing [Friend Data] with third-party applications." But as mitigation for this risk, the assessment pointed to the existence of Facebook's data use policy, which Meta knew few users read. The Privacy Risk Assessment also claimed that a list of help articles mitigated this same risk, but those articles made no mention of

app privacy settings. Importantly, those performing the risk assessment didn't appear to review the privacy settings page to look for the app privacy settings, or they may have noticed that there was no mention of apps on that page. Nor did they appear to review the new location of the app privacy settings, where they may have seen that the settings were now buried. Meta repeated its Privacy Risk Assessment exercise in 2014 and 2015 and made few changes.

38. Finally, Meta's annual review of the Privacy Risk Assessment was virtually non-existent. Meta told the FTC that its focused privacy summit would "review and update the privacy risk assessment, . . . evaluate those privacy risks, . . . [and] examine the sufficiency of existing privacy controls in mitigating those risks, as well as new potential risks." But Meta did no such thing. Participants testified that the annual risk review was nothing more than a brief and informal chat lasting less than two hours. There is no evidence that the Privacy Risk Assessment was even reviewed at the privacy summit, or that there was any discussion of the adequacy of existing controls for mitigating risk to users' privacy. Nor is there evidence that Meta discussed apps, the user interface, or privacy settings.

39. Meta's lackluster mitigation efforts not only violated the FTC order, they failed to prevent Facebook from employing a deceptive user interface. The law does not require consumers "to look beyond misleading representations on the front of a product to discover the truth from . . . the small print on the back." (*Salazar v. Walmart, Inc.* (2022) 83 Cal.App.5th 561, 567.) So too here with the user interface—Meta could not cure its deception through buried privacy settings, confusing descriptions of data sharing, or a lengthy privacy policy. Instead, when assessing privacy risks, Meta's senior leaders and privacy professionals should have evaluated the user interface through the eyes of a typical user, asking what they would have understood from the privacy settings and disclosures about third parties' access to data. This is especially so when Meta had internal and external evidence that people did not know that third-party apps stealthily collected Friend Data. Had Meta assessed the risks of the user interface in this way, and then fixed Facebook's deceptive interface and apps' access to Friend Data sooner, the company likely would have complied with the letter and intent of the FTC order and prevented the Cambridge Analytica scandal from ever happening.

FIRST CAUSE OF ACTION:
VIOLATIONS OF BUSINESS AND PROFESSIONS CODE SECTION 17500

40. The People reallege and incorporate herein by this reference paragraphs 1 through 39, inclusive. In engaging in that conduct, Meta violated California's False Advertising Law.

41. Specifically, Meta made in California, or disseminated to Californians, untrue and misleading statements concerning its services and circumstances connected with the performance of those services. Meta knew, or by the exercise of reasonable care should have known, that such statements were untrue or misleading. These statements include:

- Falsely telling users that they could limit access to their posts and data to their Friends;
- Other material misrepresentations and/or omissions regarding how the company shared a user's information with third parties;
- False or misleading statements regarding the company's knowledge of violations of its policies relating to protecting users' information and the company's efforts to enforce those policies.

42. Meta's untrue and misleading statements were likely to deceive a reasonable user and in fact did deceive millions of users in California and across the country.

SECOND CAUSE OF ACTION:
VIOLATIONS OF BUSINESS AND PROFESSIONS CODE SECTION 17200

43. The People reallege and incorporate herein by this reference paragraphs 1 through 42, inclusive. In engaging in this conduct, Meta violated California's Unfair Competition Law.

44. Specifically, Meta engaged in unlawful, unfair, or fraudulent acts or practices that constitute unfair competition as defined in Business and Professions Code section 17200. These acts or practices include acts and practices detailed above and include the following:

- False and misleading statements in violation of the False Advertising Law;
- Violations of the FTC's 2012 Order and 45 U.S.C. § 45(l), requiring Meta to implement and maintain a comprehensive privacy program that identifies and addresses material risks to users' data being disclosed and make certain disclosures when it shares users' data with third parties contrary to the users' privacy settings.

PRAYER FOR RELIEF

WHEREFORE, the People pray for judgment as follows:

45. Pursuant to Business and Professions Code sections 17203 and 17535, that Meta, its successors, agents, representatives, employees, and all persons who act in concert with them, be permanently enjoined from committing any acts that violate the Unfair Competition Law or False Advertising Law, including, but not limited to, the acts and practices alleged in this Complaint;

46. That the Court make such orders or judgments as may be necessary to prevent the use or employment by Meta, its successors, agents, representatives, employees, and all persons who act in concert with them of any practice that constitutes unfair competition or false advertising, under the authority of Business and Professions Code sections 17203 and 17535, respectively;

47. That the Court assess a civil penalty of $2,500 against Meta for each violation of Business and Professions Code section 17200 in a number according to proof, under the authority of Business and Professions Code section 17206;

48. That the Court assess a civil penalty of $2,500 against Meta for each violation of Business and Professions Code section 17500 in a number according to proof, under the authority of Business and Professions Code section 17536;

49. In addition to any penalties assessed under Business and Professions Code sections 17206 and 17536, that the Court assess a civil penalty of $2,500 against Meta for each violation of Business and Professions Code section 17200 perpetrated against a senior citizen or disabled person, in an amount according to proof, under the authority of Business and Professions Code section 17206.1;

50. That the People recover their costs of suit, including costs of investigation;

51. That the People receive all other relief to which they are legally entitled; and

52. For such other and further relief that the Court deems just and proper.

Dated: December 18, 2025

Respectfully Submitted,

ROB BONTA
Attorney General of California
NICKLAS A. AKERS
Senior Assistant Attorney General
STACEY D. SCHESSER
Supervising Deputy Attorney General

MICAH C. E. OSGOOD
MANEESH SHARMA
ANDREW J. WIENER
CAROLINE E. WILSON
Deputy Attorneys General
Attorneys for the People of the State of California

SF2018400570
43581829.docx