BURSOR & FISHER, P.A.
Sarah N. Westcot (State Bar No. 264916)
701 Brickell Ave., Suite 2100
Miami, FL 33131-2800
Telephone: (305) 330-5512
Facsimile: (305) 676-9006
Email: swestcot@bursor.com

STERLINGTON, PLLC
Arturo Peña Miranda (State Bar No. 325108)
arturo.pena@sterlingtonlaw.com
Jennifer Czeisler (*pro hac vice* forthcoming)
jen.czeisler@sterlingtonlaw.com
Edward Ciolko (*pro hac vice* forthcoming)
edward.ciolko@sterlingtonlaw.com
228 Park Ave. South, #97956
New York, New York 10003
Tel: (212) 433-2993

Counsel for Plaintiffs

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF SAN MATEO

A.A. and C.M., individually and on behalf of all others similarly situated,

Plaintiffs,

v.

META PLATFORMS, INC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs A.A. and C.M. (collectively, "Plaintiffs") bring this class action complaint on behalf of themselves and all others similarly situated (the "Class Members") against Defendant Meta Platforms, Inc. ("Defendant" or "Facebook")[1]. Plaintiffs bring this action based on personal knowledge of the facts pertaining to themselves, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

NATURE OF THE ACTION

1. This is a class action brought on behalf of all California residents who maintain a Facebook account and who accessed and used www.hellowisp.com (the "Website") to purchase over-the-counter and prescription medications.

2. The Website represents that patients can access "healthcare on your terms,"[2] and offers consumers convenient access to medications for the treatment of sexual and reproductive health issues.

3. Treatment related to sexual and reproductive health is inherently personal, involving intimate details about an individual's health and reproductive choices. When seeking such treatment, patients reasonably expect that information related to their medical treatment will be kept confidential and not intercepted and recorded by unknown third parties.

4. Such expectations are based, in part, on the legal protections afforded to such information.

5. Despite these protections, Facebook intentionally intercepted this protected information through tacking technology embedded on the Website, including its software development kits ("SDK") and tracking pixel.

6. The protected information intercepted by Facebook was not aggregated or deidentified. More troubling is the fact that Facebook used this information for its own purposes, including targeted advertising.

7. Plaintiffs and class members provided their personal information, including health

[1] In October 2021, Facebook, Inc. changed its name to Meta Platforms, Inc. Unless otherwise indicated, Facebook, Inc. and Meta Platforms, Inc. are referenced collectively as "Facebook."

[2] WISP, https://hellowisp.com/about.

conditions for which they were seeking treatment, when browsing for and purchasing medications on the Website with the expectation that this information would remain confidential and private. Defendant's unlawful interception and recording of this information without explicit consent constitutes an extreme invasion of Plaintiffs' and Class members' privacy. Plaintiffs bring this action for legal and equitable remedies resulting from these illegal actions.

PARTIES

8. Plaintiff A.A. is a California citizen who resides in San Diego, California. On August 25, 2023, Plaintiff A.A. was prescribed and ordered Norethindrone birth control medication through the Website. Unbeknownst to Plaintiff A.A., Facebook intercepted and recorded protected health information ("PHI") related to her prescription medication through proprietary software codes, as described more thoroughly below. Due to the surreptitious nature of the interceptions at issue, Plaintiff A.A. did not realize confidential information related to this medical prescription was intercepted and recorded by Facebook until August 19, 2024. Plaintiff A.A. was in California when she ordered prescription medication through the website.

9. Plaintiff C.M. is a California citizen who resides in Siskiyou County, California. From approximately 2022 through 2024, Plaintiff C.M. accessed the Website to book medical appointments, look up medical information, and buy prescription medications. For example, on March 7, 2022 Plaintiff C.M. attended a telehealth appointment via the Website to consult with a healthcare professional about her sensitive health condition. Later that day, she purchased Metronidazole, the prescribed medication, through the Website. Plaintiff C.M. last visited the Website on June 10, 2024, when she attended another telehealth appointment. As before, she purchased Norethisterone, the prescribed medication, through the Website later that day.

10. Unbeknownst to Plaintiff C.M., Facebook intercepted her confidential prescription information through software code known as the Facebook Tracking Pixel, as described below. Due to the surreptitious nature of the interceptions at issue, Plaintiff C.M. did not realize information related to her prescription was intercepted and recorded by Facebook until around October 2024. Plaintiff C.M. was in California when she ordered prescription medication through the Website.

11. During the time Plaintiffs accessed and used the Website, they each maintained an active social media account with Facebook. Plaintiffs used the same device to access the Website and their Facebook account. Subsequently, as a result of the conduct of the Defendant, Plaintiffs both received targeted advertisements on Facebook relating to sexual and reproductive health medications.

12. Facebook committed the interceptions at issue without Plaintiffs' knowledge, consent, or express written authorization.

13. Such acts are egregious violations of Plaintiffs' right to privacy.

14. Defendant, Meta Platforms, Inc., is a Delaware corporation with its principal place of business located in Menlo Park, California. Facebook at all times knew that the incorporation of its software into the Website would result in its interception of PHI and other sensitive data. Facebook, as the creator of its software and the Facebook Tracking Pixel, knew that it intercepted each of a users' interactions on the Website that incorporated its technology. Facebook has consistently come under scrutiny for incorporating its technology on websites that involve the transmittal of sensitive data, including health information, but continues to do so because of the value of the health information it intercepts for targeted advertising.

15. As demonstrated by the continued incorporation of the Facebook Tracking Pixel on the Website, Facebook did not take any steps to prevent its interception and use of the Website's patient's sensitive health data.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action pursuant to Article VI, section 10 of the California Constitution and California Code of Civil Procedure section 382.

17. This Court has personal jurisdiction over Defendant pursuant to California Code of Civil Procedure section 410.10 because Defendant conducts substantial business such that Defendant has significant, continuous, and pervasive contacts with the State of California and because Defendant resides in California.

18. This Court is the proper venue for this action under the California Code of Civil Procedure section 395.5 because the conduct alleged ion this complaint occurred in this county and

Defendant resides in this county.

FACTUAL ALLEGATIONS

A. Facebook Intercepted Sensitive, Private Information

19. Defendant intercepted information that was sensitive, private, and personally identifiable.

20. Americans have an expectation of privacy when it concerns reproductive health information. This is especially true when the disclosure of such information can reveal an individual's sexual preferences, sexual orientation, and/or pregnancy status.

21. Not only is this confidential and sensitive, but it is also legally protected. In 2020, California passed the California Privacy Rights Act, which expands the protections afforded by the California Consumer Privacy Act. This includes expanding the term "sensitive personal information" to include "[p]ersonal information collected and analyzed concerning a consumer's sex life or sexual orientation." Cal. Civ. Code § 1798.140(ae)(2)(C).

22. Further, the information Facebook intercepted is also protected by California's Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code § 56.

23. The CMIA prohibits "[a] provider of health care . . . [from disclosing] medical information regarding a patient of the provider of health care . . . without first obtaining an authorization." Cal. Civ. Code § 67.10(a).

24. Wisp qualifies as a "provider of health care" under CMIA.

25. "Medical information" is defined as:

> [A]ny individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental health application information, **reproductive or sexual health application information**, mental or physical condition, or treatment. "Individually identifiable" means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the identity of the individual.

Cal. Civ. Code § 56.05(j) (emphasis added).

26. "Reproductive or sexual health application information" is defined as:

> [I]nformation about a consumer's reproductive health, menstrual cycle, fertility, pregnancy, pregnancy outcome, plans to conceive, or type of sexual activity collected by a reproductive or sexual health digital service, including, but not limited to, information from which one can infer someone's pregnancy status, menstrual cycle, fertility, hormone levels, birth control use, sexual activity, or gender identity.

Cal. Civ. Code § 56.05(q).

B. Facebook's Platform and Business Tools

27. Facebook describes itself as a "real identity platform,"[3] meaning users are allowed only one account and must share "the name they go by in everyday life."[4] To that end, when creating an account, users must provide their first and last name, along with their birthday and gender.[5]

28. In 2023, Facebook generated over $134 billion in revenue.[6] With respect to the apps offered by Facebook, substantially all of Facebook's revenue is generated by selling advertising space.[7]

29. Facebook sells advertising space by highlighting its ability to target users.[8] Facebook can target users effectively because it surveils user activity on and off its site.[9] This allows Facebook to make inferences about users beyond what they explicitly disclose, like their

---

[3] Sam Schechner & Jeff Horwitz, *How Many Users Does Facebook Have? The Company Struggles to Figure It Out*, WALL ST. J. (Oct. 21, 2021, 4:05 PM), https://www.wsj.com/articles/how-many-users-does-facebook-have-the-company-struggles-to-figure-it-out-11634846701.

[4] FACEBOOK, COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY, https://www.facebook.com/communitystandards/integrity_authenticity.

[5] FACEBOOK, SIGN UP, https://www.facebook.com.

[6] FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2023 RESULTS; INITIATES QUARTERLY DIVIDEND, https://s21.q4cdn.com/399680738/files/doc_news/Meta-Reports-Fourth-Quarter-and-Full-Year-2023-Results-Initiates-Quarterly-Dividend-2024.pdf at 8.

[7] *Id.*

[8] FACEBOOK, WHY ADVERTISE ON FACEBOOK, INSTAGRAM AND OTHER META TECHNOLOGIES, https://www.facebook.com/business/help/205029060038706.

[9] FACEBOOK, ABOUT META PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142.

"interests," "behavior," and "connections."[10] Facebook compiles this information into a generalized dataset called "Core Audiences," which allows advertisers to reach precise audiences based on specified targeting types.[11]

30. Advertisers can also build "Custom Audiences."[12] Custom Audiences enables advertisers to reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website."[13] With Custom Audiences, advertisers can target existing customers directly and build "Lookalike Audiences," which "leverage[] information such as demographics, interests and behaviors from your source audience to find new people who share similar qualities."[14] Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if they first supply Facebook with the underlying data. They can do so through two mechanisms: (1) by manually uploading contact information for customers or (2) by utilizing Facebook's "Business Tools."[15]

31. As Facebook puts it, the Business Tools "help website owners and publishers, app developers, and business partners, including advertisers and others, integrate with [Facebook], understand and measure their products and services, and better reach and serve people who might be interested in their products and services."[16] Put more succinctly, Facebook's Business Tools are bits of code that advertisers can integrate into their websites, mobile applications, and servers, thereby enabling Facebook to intercept and collect user activity on those platforms.

32. The Business Tools are automatically configured to capture certain data, like when a

---

[10] FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting.

[11] FACEBOOK, https://www.facebook.com/business/news/Core-Audiences.

[12] FACEBOOK, ABOUT CUSTOM AUDIENCES, https://www.facebook.com/business/help/744354708981227?id=2469097953376494.

[13] FACEBOOK, AUDIENCE AD TARGETING, https://www.facebook.com/business/ads/ad-targeting.

[14] FACEBOOK, ABOUT LOOKALIKE AUDIENCES, https://www.facebook.com/business/help/164749007013531?id=401668390442328.

[15] FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, https://www.facebook.com/business/help/170456843145568?id=2469097953376494; FACEBOOK, CREATE A WEBSITE CUSTOM AUDIENCE, https://www.facebook.com/business/help/1474662202748341?id=2469097953376494.

[16] FACEBOOK, THE META BUSINESS TOOLS, https://www.facebook.com/help/331509497253087.

user visits a webpage, that webpage's Universal Resource Locator ("URL") and metadata, or when a user downloads a mobile application or makes a purchase.[17] Facebook's Business Tools can also track other events. Facebook offers a menu of "standard events" from which advertisers can choose, including what content a visitor views or purchases.[18] Advertisers can even create their own tracking parameters by building a "custom event."[19]

33. One such Business Tool is the Facebook Tracking Pixel. Facebook encourages advertisers, like Wisp, to integrate this software into their website. As the name implies, the Facebook Tracking Pixel "tracks the people and type of actions they take."[20] When a user accesses a website hosting the Facebook Tracking Pixel, Facebook's software script surreptitiously directs the user's browser to contemporaneously send a separate message to Facebook's servers. This second secret and contemporaneous transmission contains the original GET request sent to the host website, along with additional data that the Facebook Tracking Pixel is configured to collect. This transmission is initiated by Facebook code and concurrent with the communications with the host website. At relevant times, two sets of code were thus automatically run as part of the browser's attempt to load and read the Website—Wisp's own code and Facebook's embedded code.

34. Facebook's own documentation makes clear how extensively the Facebook Tracking Pixel tracks private information. It describes the Facebook Tracking Pixel as code that Facebook's business customers can put on their website to "[m]ake sure your ads are shown to the right people[] [and] ***[f]ind . . . people who have visited a specific page or taken a desired action on***

---

[17] *See* FACEBOOK, META FOR DEVELOPERS: META PIXEL, ADVANCED, https://developers.facebook.com/docs/meta-pixel/advanced/; *see also* FACEBOOK, BEST PRACTICES FOR META PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; FACEBOOK, META FOR DEVELOPERS: MARKETING API - APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

[18] FACEBOOK, SPECIFICATIONS FOR META PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142.

[19] FACEBOOK, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* FACEBOOK, META FOR DEVELOPERS: MARKETING API – APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

[20] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting.

your website" (emphasis added).[21]

35. Facebook instructs such business customers that:

> Once you've set up the [Facebook Tracking] Pixel, ***the pixel will log when someone takes an action on your website***. Examples of actions include adding an item to their shopping cart or making a purchase. ***The Pixel receives these actions, or events***, which you can view on your [Facebook Tracking] Pixel page in Events Manager. From there, you'll be able to see the actions that your customers take. ***You'll also have options to reach those customers again through future Meta ads***.[22]

36. This tracked information includes private data revealing prescribed medications purchased by consumers on the Website.

37. The Facebook Tracking Pixel code enables Facebook not only to help Wisp with advertising to its own patients outside the Website, but also includes individual patients among groups targeted by ***other*** Facebook advertisers relating to the conditions about which patients communicated on the Website.

38. Facebook's Business Help Center explains:

> Meta ***uses event data to show ads to people who are likely to be interested in them***. One type of marketing data is website events, which are ***actions that people take on your website***.[23]

39. In other words, Facebook sells advertising space by highlighting its ability to target users.[24] Facebook can target users so effectively because it surveils user activity both on and off its site.[25] This allows Facebook to make inferences about users beyond what they explicitly disclose, like their "interests," "behaviors," and connections.[26]

40. An example illustrates how the Facebook Tracking Pixel works. Take an individual

---

[21] META, ABOUT META PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142.

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

[23] META, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142 (emphasis added).

[24] META, WHY ADVERTISE ON FACEBOOK, INSTAGRAM AND OTHER META TECHNOLOGIES, https://www.facebook.com/business/help/205029060038706 (last visited May 21, 2024).

[25] META, ABOUT META PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142.

[26] META, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting.

who, at relevant times, navigated to the Website and clicked on a link to purchase prescription medication. When that link was clicked, the individual's browser sent a GET request to Wisp's servers requesting the servers to load the particular webpage. Facebook's embedded code, written in JavaScript, then sent secret instructions back to the individual's browser, without alerting the individual that this was happening. Facebook caused the browser to secretly duplicate the communication with Wisp, transmitting it to Facebook's servers, alongside additional information that transcribed the communication's content and the individual's identity.

41. Examples of these interceptions from the Website are provided in Figures 1 and 2 below:

Figure 1:


```
"status": "COMPLETE",
"method": "GET",
"protocolVersion": "HTTP/2.0",
"scheme": "https",
"host": "www.facebook.com",
"actualPort": 443,
"path": "/tr/",
"query": "id=253897343916108&ev=AddToCart&dl=https%3A%2F%2Fhellowisp.com%2Fproducts%2Ftri-sprintec-birth-control%3Fflow%3Dopen&rl=&if=false&ts=1713302543539&cd[content_type]=product&cd[content_ids]=%5B%22LO_A_OT_LP%22%2C%22HL2-OT-SH%22%2C%22TSP3-SUB-SH%22%2C%22OM1-A-SUB-SH%22%5D&cd[value]=158.66&cd[currency]=USD&sw=1920&sh=1080&v=2.9.153&r=stable&a=tmSimo-GTM-WebTemplate&ec=13&o=4126&fbp=fb.1.1713302395193.221102072&ler=empty&cdl=API_unavailable&it=1713302395143&coo=false&tm=1&rqm=GET",
"tunnel": false,
"keptAlive": true,
"webSocket": false,
"remoteAddress": "www.facebook.com/31.13.67.35",
"clientAddress": "/127.0.0.1",
"clientPort": 53981,
"times": {
    "start": "2024-04-16T17:22:23.355-04:00",
    "requestBegin": "2024-04-16T17:22:23.355-04:00",
    "requestComplete": "2024-04-16T17:22:23.356-04:00",
    "responseBegin": "2024-04-16T17:22:23.364-04:00",
```


Figure 2:


```
"name": ":method",
"value": "GET"
},
{
"name": ":authority",
"value": "www.facebook.com"
},
{
"name": ":scheme",
"value": "https"
},
{
"name": ":path",
"value": "/tr/?id=1863436503950868&ev=SubscribedButtonClick&dl=https%3A%2F%2Fhellowisp.com%2Fcheckout&rl=&if=false&ts=1713303085392&sw=1920&sh=1080&udff[em]=fcb1303ed96777298d2f4ee5aba933364beb5028c502d111517c022cb9[illegible]d644f40bdcc8f7ae00e89a4ae4fbc44031c4bc27e54dd4bcb9773&udff[ln]=c1d35cc3471fe509203d65b3e7a53fc82337ac9ae2c797b836621f706fe37df8&udff[ph]=4b46886d094c51dd5db53e610d6e652d322b29097dfb316eb1c1bb358d65952e&udff[ct]=c55ec4bbe9c7c1614204f286194b109010ca0680f41325ec1a82302a34b4f3f7&udff[zp]=3fa77ea8f0527c6f0419f4eb9bae514e94a0f190a4a7e84a59f6f44a3c922551&v=2.9.153&r=stable&a=tmSimo-GTM-WebTemplate&ec=52&o=7198&fbp=fb.1.1713302395193.221102072&ler=empty&cdl=API_unavailable&it=1713302395143&coo=false&es=automatic&tm=3&rqm=GET"
},
{
"name": "sec-ch-ua",
"value": "\"Google Chrome\";v=\"123\", \"Not:A-Brand\";v=\"8\", \"Chromium\";v=\"123\""
},
{
"name": "sec-ch-ua-mobile",
"value": "?0"
```

42. Through the Facebook Tracking Pixel, Defendant intercepted and recorded "AddtoCart" and "SubscribedButtonClick" events, which detail information about which products the patient was purchasing on the website.

43. Specifically, when a consumer purchases birth control products from the Website, the AddToCart even information shared with Facebook the terms "hellowisp," "birthcontrol," and "tri-sprintec." *See* Figure 1.

44. Similar data is intercepted by Facebook when a patient completes the checkout process on the Website through the "SubscribedButtonClick" event, notifying Facebook that the medication was purchased. *See* Figure 2.

45. Each time Facebook intercepted this activity data through the Facebook Tracking Pixel, it also disclosed a patient's personally identifiable information, including their Facebook ID ("FID"). An FID is a unique and persistent identifier that Facebook assigns to each user. With it, any ordinary person can look up the user's Facebook profile and name. Notably, while Facebook can easily identify any individual on its Facebook platform with only their unique FID, so too can any ordinary person who comes into possession of an FID. Facebook admits as much on its website. Indeed, ordinary people who come into possession of the FID can connect to any Facebook profile.

46. A user who accessed the Website while logged into Facebook transmitted what is known as a "c_user cookie" to Facebook, which contains that user's unencrypted FID.

47. When a visitor's browser had recently logged out of an account, Facebook compelled the visitor's browser to send a smaller set of cookies.

48. One such cookie was the "fr cookie" which contained, at least, an encrypted FID and browser identifier.[27] Facebook, at a minimum, used the fr cookie to identify users.[28]

49. If a visitor had never created an account, an even smaller set of cookies was transmitted.

---

[27] DATA PROTECTION COMMISSIONER, FACEBOOK IRELAND LTD, REPORT OF RE-AUDIT (Sept. 21, 2012), http://www.europe-v-facebook.org/ODPC_Review.pdf.

[28] FACEBOOK, PRIVACY CENTER – COOKIES POLICY, https://www.facebook.com/privacy/policies/cookies/?subpage=subpage-1.3.

50. At each stage, the Website utilized the "_fbp cookie," which attached to a browser as a first-party cookie, and which Facebook used to identify a browser and a user.[29]

51. The c_user cookie expires after 90 days if the user checked the "keep me logged in" checkbox on the website.[30] Otherwise, the c_user cookie is cleared when the browser exits.[31]

52. The fr cookie expires after 90 days unless the visitor's browser logs back into Facebook.[32] If that happens, the time resets, and another 90 days begins to accrue.[33]

53. The _fbp cookie expires after 90 days unless the visitor's browser accesses the same website.[34] If that happens, the time resets, and another 90 days begins to accrue.[35]

54. The Facebook Tracking Pixel used both first- and third-party cookies. A first-party cookie is "created by the website the user is visiting"—*i.e.*, Wisp's Website.[36] A third-party cookie is "created by a website with a domain name other than the one the user is currently visiting"—*i.e.*, Facebook.[37] The _fbp cookie was always transmitted as a first-party cookie. A duplicate _fbp cookie was sometimes sent as a third-party cookie, depending on whether the browser had recently logged into Facebook.

55. Facebook, at a minimum, used the fr, _fbp, and c_user cookies to link to FIDs and corresponding Facebook profiles. Wisp sent these identifiers alongside the event data.

56. Plaintiffs' offsite activity report from their personal Facebook account confirms that their sensitive, confidential, and protected information was intercepted by Facebook through the

---

[29] *Id.*

[30] Seralthan, FACEBOOK COOKIES ANALYSIS (Mar. 14, 2019), https://techexpertise.medium.com/facebook-cookies-analysis-e1cf6ffbdf8a.

[31] *Id.*

[32] *See id.*

[33] Confirmable through developer tools.

[34] FACEBOOK, PRIVACY CENTER – COOKIES POLICY, https://mbasic.facebook.com/privacy/policies/cookies/printable/#annotation-1.

[35] Also confirmable through developer tools.

[36] PC MAG, FIRST-PARTY COOKIE, https://www.pcmag.com/encyclopedia/term/first-party-cookie. This is confirmable by using developer tools to inspect a website's cookies and track network activity.

[37] PC MAG, THIRD-PARTY COOKIE, https://www.pcmag.com/encyclopedia/term/third-party-cookie. This is also confirmable by tracking network activity.

Website.

57. Alternatively, Facebook can also match this prescription information to the specific Wisp patient based on the PII intercepted from the patient's medical profile.

58. After collecting and intercepting the information described in the preceding paragraphs, Facebook processed, analyzed, and assimilated it into datasets like Core Audiences and Custom Audeinces.

59. Plaintiffs never consented, agreed, authorized, or otherwise permitted Facebook to disclose their PII and PHI.

60. By law, Plaintiffs are entitled to privacy in their protected health information and confidential communications. Facebook deprived Plaintiffs of their privacy rights when they: (1) implemented a system that surreptitiously tracked, recorded, and disclosed Plaintiffs' and other online patients' confidential communications, personally identifiable information, and protected health information; (2) disclosed and/or intercepted patients' protected health information; and (3) undertook this pattern of conduct without notifying Plaintiffs and without obtaining their express written consent.

D. Tolling

61. Any applicable statutes of limitations have been tolled by Defendant's knowing and active concealment of its interception and recording of legally protected information.

62. The Facebook Tracking Pixel, discussed *supra*, was and is entirely invisible to a website visitor.

63. Through no fault or lack of diligence, Plaintiffs and Class members were deceived and could not reasonably discover Defendant's deception and unlawful conduct.

64. Plaintiffs were ignorant of the information essential to pursue their claims, without any fault or lack of diligence on their part.

65. Defendant had exclusive knowledge that its tracking technology was incorporated into the Website and yet failed to disclose to its account holders, including Plaintiffs and Class members, that by purchasing medication through the Website, Plaintiff's and Class members' PII and PHI would be intercepted and recorded by Facebook for targeted advertising.

66. Under the circumstances, Defendant was under a duty to disclose the nature, significance, and consequences of its collection of its account holders' PII and PHI. In fact, to the present, Defendant has not conceded, acknowledged, or otherwise indicated to its account holders that it has unlawfully intercepted and recorded their PII and PHI. Accordingly, Defendant is estopped from relying on any statute of limitations.

67. Moreover, all applicable statutes of limitations have also been tolled pursuant to the discovery rule.

68. The earliest that Plaintiffs or Class members, acting with due diligence, could have reasonably discovered Defendant's conduct would have been shortly before the filing of the Plaintiffs' complaint in this matter.

69. Plaintiffs first discovered that Defendant had intercepted and recorded their PII and PHI after contacting undersigned counsel and discussing potential claims against Defendant.

CLASS ACTION ALLEGATIONS

70. Class Definition: Pursuant to Cal. Code Civ. Proc. § 382, Plaintiffs bring this action on behalf of themselves and other similarly situated individuals defined as all persons in the state of California who, during the class period, had their personally identifiable information or protected health information intercepted and recorded by Facebook while purchasing products on the Website (the "Class").

71. Plaintiffs reserve the right to modify the class definitions or add sub-classes as necessary prior to filing a motion for class certification.

72. The "Class Period" is the time period beginning on the date established by the Court's determination of any applicable statute of limitations, after consideration of any tolling, concealment, and accrual issues, and ending on the date of entry of judgement.

73. Excluded from the Class is the Defendant; any affiliate, parent, or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any officer, director, or employee of Defendant; any successor or assign of Defendant; anyone employed by counsel in this action; any judge to whom this case is assigned, his/her spouse and immediate family members; and members of the judge's staff.

74. Numerosity. Members of the Class are so numerous that joinder of all members is impracticable. The exact number of Class Members is unknown to Plaintiffs at this time; however, it is estimated that there are at least thousands of individuals in the Class. The identity of such membership is readily ascertainable from Defendant's records.

75. Typicality. Plaintiffs' claims are typical of the claims of the Class because Plaintiffs used hellowisp.com to purchase prescription medications and had their personally identifiable information and protected health information disclosed to Facebook without their express written authorization or knowledge. Plaintiffs' claims are based on the same legal theories as the claims of other Class Members.

76. Adequacy. Plaintiffs are prepared to take all necessary steps to represent fairly and adequately the interests of the Class Members. Plaintiffs' interests are coincident with, and not antagonistic to, those of the members of the Class. Plaintiffs are represented by attorneys with experience in the prosecution of class action litigation, generally, and in the emerging field of digital privacy litigation, specifically. Plaintiffs' attorneys are committed to vigorously prosecuting this action on behalf of the members of the Class.

77. Commonality. Questions of law and fact common to the members of the Class predominate over questions that may affect only individual members of the Class because Defendant has acted on grounds generally applicable to the Class. Such generally applicable conduct is inherent in Defendant's wrongful conduct. Questions of law and fact common to the Class include:

a. Whether Defendant intentionally tapped the lines of internet communication between patients and their healthcare provider;

b. Whether Defendant surreptitiously recorded personally identifiable information, protected health information, and related communications on the Website;

c. Whether Defendant is a third-party eavesdropper;

d. Whether Defendant's interception of personally identifiable information, protected health information, and related communications constituted an affirmative act of communication;

e. Whether Defendant violated Plaintiffs' and Class Members' privacy rights by using the Facebook Tracking Pixel to record and communicate patients' confidential medical communications;

f. Whether Plaintiffs and Class members are entitled to damages under the CIPA, or any other relevant statute; and

g. Whether Defendant's actions violated Plaintiffs' and Class Members' privacy rights as provided by the California Constitution.

78. Superiority. Class action treatment is the superior method for the fair and efficient adjudication of this controversy. Such treatment permits a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons or entities a method for obtaining redress on claims that could not practicably be pursued individually, substantially outweigh any potential difficulties in the management of this class action. Plaintiffs know of no special difficulty to be encountered in litigating this action that would preclude its maintenance as a class action.

COUNT I
Violation of the California Invasion of Privacy Act,
Cal. Penal Code § 632

79. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein and bring this count individually and on behalf of the members of the Class against Defendant.

80. Cal. Penal Code § 632 prohibits "intentionally and without the consent of all parties to a confidential communication," the "use[] [of] an electronic amplifying or recording device to eavesdrop upon or record the confidential communication". .

81. Section 632 defines "confidential communication" as "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto[.]"

82. Plaintiffs' and Class Members' communications to Wisp, including their sensitive

personal and health information, such as information related to their prescription medications, were confidential communications for purposes of § 632, because Plaintiffs and Class Members had an objectively reasonable expectation of privacy in this data.

83. Plaintiffs and Class Members expected their communications to Wisp to be confined to Wisp due to the confidential nature of those communications. Plaintiffs and Class Members did not expect third parties, specifically Facebook, to secretly eavesdrop upon or record this information and their communications.

84. Facebook's tracking technology, i.e., the Facebook Tracking Pixel, is an electronic amplifying or recording devices for purposes of § 632.

85. By contemporaneously intercepting and recording Plaintiffs' and Class Members' confidential communications to Wisp through this technology, Facebook eavesdropped and/or recorded confidential communications through an electronic amplifying or recording device in violation of § 632 of CIPA.

86. At no time did Plaintiffs or Class Members consent to Facebook's conduct, nor could they reasonably expect that their communications to Wisp would be overheard or recorded by Facebook.

87. Facebook utilized Plaintiffs' and Class Members' sensitive personal and health information for their own purposes, including for targeted advertising.

88. Plaintiffs and Class Members seek statutory damages in accordance with § 637.2(a) which provides for the greater of: (1) $5,000 per violation; or (2) three times the amount of damages sustained by Plaintiffs and the members of the Class in an amount to be proven at trial, as well as injunctive or other equitable relief.

89. Plaintiffs and members of the Class have also suffered irreparable injury from these unauthorized acts. Plaintiffs' and Class Members' sensitive data has been collected, viewed, accessed, stored, by Facebook, have not been destroyed, and due to the continuing threat of such injury, have no adequate remedy at law. Plaintiffs and Class Members are accordingly entitled to injunctive relief.

COUNT II
Invasion of Privacy Under California's Constitution

90. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein and bring this count individually and on behalf of the members of the Class against Defendant.

91. Plaintiffs and Class Members have an interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential communications and protected health information; and (2) making personal decisions and/or conducting personal activities without observation, intrusion, or interference, including, but not limited to, the right to visit and interact with various internet sites without being subjected to wiretaps without Plaintiffs' and Class Members' knowledge or consent.

92. At all relevant times, by using the SDKs and other software codes to record and communicate patients' personal identifiers alongside their confidential medical communications, Facebook intentionally invaded Plaintiffs' and Class Members' privacy rights under the California Constitution.

93. Plaintiffs and Class Members had a reasonable expectation that their communications, identities, health information, and other data would remain confidential.

94. Plaintiffs and Class Members did not authorize Defendant to record and transmit Plaintiffs' and Class Members' private medical communications alongside their personally identifiable and health information.

95. This invasion of privacy was serious in nature, scope, and impact because it related to patients' private medical communications. Moreover, it constituted an egregious breach of the societal norms underlying the privacy right.

96. Accordingly, Plaintiffs and members of the Class seek all relief available for invasion of privacy under the California Constitution.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for relief and judgment, as follows:

a. For a determination that this action is a proper class action;

b. For an order certifying the Class, naming Plaintiffs as representatives of the Class, and naming Plaintiffs' attorneys as Class Counsel to represent the Class;

c. For an order declaring that Defendant's conduct violated the statutes referenced herein;

d. For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

e. For an award of compensatory damages, including statutory damages where available, to Plaintiffs and the Class Members against Defendant for all damages sustained as a result of Defendant's wrongdoing, in an amount to be proven at trial;

f. For punitive damages, as warranted, in an amount to be determined at trial;

g. For an order requiring Defendant to disgorge revenues and profits wrongfully obtained;

h. For prejudgment interest on all amounts awarded;

i. For injunctive relief as pleaded or as the Court may deem proper;

j. For an order awarding Plaintiffs and the Class their reasonable attorneys' fees and expenses and costs of suit; and

k. For an order granting Plaintiffs and Class Members such further relief as the Court deems appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the proposed Class, demand a trial by jury for all of the claims asserted in this Complaint so triable.

Dated: August 12, 2025

Respectfully submitted,

BURSOR & FISHER, P.A.

By: Sarah N. Westcot

Sarah N. Westcot

Sarah N. Westcot (State Bar No. 264916)
701 Brickell Ave., Suite 2100
Miami, FL 33131-2800
Telephone: (305) 330-5512
Facsimile: (305) 676-9006
Email: swestcot@bursor.com

STERLINGTON, PLLC
Arturo Peña Miranda (State Bar No. 325108)
arturo.pena@sterlingtonlaw.com
Jennifer Czeisler (*pro hac vice* forthcoming)
jen.czeisler@sterlingtonlaw.com
Edward Ciolko (*pro hac vice* forthcoming)
edward.ciolko@sterlingtonlaw.com
228 Park Ave. South, #97956
New York, New York 10003
Tel: (212) 433-2993

Counsel for Plaintiffs