MILBERG COLEMAN BRYSON PHILLIPS
GROSSMAN, PLLC
JOHN J. NELSON (SBN 317598)
jnelson@milberg.com
280 South Beverly Drive, Penthouse
Beverly Hills, California 90212
Tel: 872.365.7060

Attorney for Plaintiff and the Class

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

VALERIE TORRES, on behalf of herself and all others similarly situated,

Plaintiff,

v.

POLICYGENIUS, LLC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT FOR:

1. **CAL. PENAL CODE § 630, *et seq.***
2. **CAL. CONST. ART. 1 § 1**
3. **INTRUSION UPON SECLUSION**
4. **BUS. & PROF. CODE § 17200**
5. **18 U.S.C. § 2511(1) *et seq*.**
6. **UNJUST ENRICHMENT**

Plaintiff Valerie Torres ("Plaintiff") brings this class action complaint individually and on behalf of all others similarly situated ("Class Members") against Policygenius, LLC ("Policygenius" or "Defendant"). The allegations contained in this class action complaint are based on Plaintiff's personal knowledge of facts pertaining to herself and upon information and belief, including further investigation conducted by Plaintiff's counsel.

NATURE OF THE ACTION

1. This is a class action lawsuit brought to address Defendant's improper and illegal disclosure of consumers' personally identifiable information ("PII") and/or protected health information ("PHI") (collectively referred to as "Private Information") to Meta Platforms, Inc. d/b/a Meta ("Facebook" or "Meta") and other third parties as a result of their use of Defendant's website, www.policygenius.com ("Website").

2. Information about a person's physical, mental, and financial health is among the most confidential and sensitive information in our society, and the mishandling of such information can have serious consequences, including discrimination in the workplace or denial of insurance coverage.

3. Defendant owns and controls www.policygenius.com, wherein customers are asked to communicate highly personal and sensitive information in order to obtain quotes for various types of life insurance and disability insurance.

4. At the outset, Policygenius assures Website users that their information will be kept confidential, and the phrase "Your information is kept secure" appears next to an

image of a padlock on the Website's homepage. The same phrase appears when users navigate to the Policygenius life insurance questionnaire within the Website. Likewise, if a user applies for disability insurance, the first page of that web survey states "We don't sell your personal information to third parties."

5. Despite these representations, Defendant intentionally installed a tracking pixel (the "Facebook Tracking Pixel" or "Pixel") on its Website to surreptitiously duplicate and send its customers' private communications to Facebook, the contents of which include Private Information and protected PHI/individually identifiable medical information.

6. By installing, programming, and controlling the Pixel as described herein, Defendant aided, agreed, employed, and conspired with Facebook to intercept Plaintiff's and Class Members' sensitive and private communications without their knowledge or consent.

7. A pixel is a piece of code that "tracks the people and [the] type of actions they take"[1] as they interact with a website, including how long a person spends on a particular web page, which buttons the person clicks, which pages they view, and the text or phrases they type into various portions of the website (such as a general search bar, chat feature, or text box), among other things.

[1] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited November 27, 2023).

8. The Pixel is programmable, meaning that the Defendant is responsible for determining which communications with the Website are tracked and transmitted to Facebook.

9. Pixels are routinely used to target specific customers by utilizing data to build profiles for the purposes of retargeting and future marketing. Upon information and belief, Defendant utilized the Pixel data for marketing and retargeting purposes in an effort to bolster its profits.

10. Correspondingly, Defendant exploits the Private Information Plaintiff and Class Members communicated to Defendant while seeking insurance coverage and uses this Private Information to create detailed profiles that reflect individual consumer preferences, allowing Facebook and Defendant to deliver targeted advertisements.

11. Defendant's website, and more specifically its source code, manipulated Plaintiff's and Class Members' web browsers so that their communications to Defendant were automatically, contemporaneously, jointly, and surreptitiously sent to Facebook—an unintended third-party recipient.

12. This is the functional equivalent of placing a bug or listening device on a phone line because Defendant's website allows third-parties to "listen in" and receive communications in real time that Plaintiff intended only for Defendant.

13. Importantly, Facebook would not receive these communications but for Defendant's installation and implementation of the Pixel.

14. In addition to the Facebook Pixel, Defendant also installed and implemented Facebook's other Business Tools, such as the Conversions Application Programming Interface ("Conversions API" or "CAPI"), on its Website.[2]

15. Unlike the Facebook Pixel, which co-opts a website user's browser and forces it to transmit information to Facebook in addition to the website owner, Conversions API does not cause the user's browser to transmit information directly to Facebook. Instead, Conversions API tracks the user's website interactions, including Private Information, records and stores that information on the website owner's servers, and then transmits the data to Facebook from the website owner's servers. [3,4] Indeed, Facebook markets Conversions API as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."[5]

[2] "CAPI works with your Facebook pixel to help improve the performance and measurement of your Facebook ad campaigns." *See* https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited: November 27, 2023).

[3] https://revealbot.com/blog/facebook-conversions-api/ (last visited: November 27, 2023).

[4] "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel…. This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels.", https://developers.facebook.com/docs/marketing-api/conversions-api (last visited: November 27, 2023).

[5] https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited: November 27, 2023).

16. Because Conversions API is located on the website owner's servers and is not a bug planted onto the website user's browser, it allows website owners like Defendant to circumvent any ad blockers or other denials of consent by the website user that would prevent the Pixel from sending website users' Private Information to Facebook directly.

17. Plaintiff reasonably believed that Policygenius would maintain the confidentiality of her Private Information and not share such information with Facebook, a social media giant with a track record of disregarding privacy rights.

18. Plaintiff and California residents were harmed by Defendant's conduct and seek relief as alleged herein.

JURISDICTION AND VENUE

19. The Court has jurisdiction over this action pursuant to 28 U.S.C § 1332(d)(2)(A) as modified by the Class Action Fairness Act of 2005 because at least one member of the Class, as defined herein, is a citizen of a different state than Policy Genius, there are more than 100 member of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

20. This Court has personal jurisdiction over Policygenius LLC because it regularly conducts business and is licensed to do business in the state of California.

21. Venue is proper in this District pursuant to 28 U.S.C § 1391 because the wrongful conduct giving rise to this case occurred in, was directed to, and/or emanated

from this District. Plaintiff resides in this District, used defendant's Website in this District, and her confidential communications were intercepted in this District.

THE PARTIES

Plaintiff Valerie Torres

22. Plaintiff Torres is an adult citizen of the state of California and is domiciled in Los Angeles, California.

23. In or about June 2022, Plaintiff Torres accessed www.policygenius.com from her mobile device and used the website to search for life insurance quotes. In doing so, Plaintiff provided Policygenius with her PII and health information. Plaintiff reasonably expected that her communications with Policygenius via its website were confidential, solely between herself and Policygenius, and that such communications would not be transmitted to or intercepted by a third party.

24. Plaintiff Torres has an active Facebook account she regularly accesses using her mobile device. As described herein, Policygenius sent Plaintiff's sensitive and private PII and health information to third parties, including Facebook, when she accessed Policygenius's website. Additionally, the information Policygenius sent to third parties was linked to Plaintiff's Facebook ID.

25. Pursuant to the systematic process described herein, Policygenius assisted third parties, including Facebook, with intercepting Plaintiff's communications, including those that contained PII, protected health information, and related confidential information.

Policygenius assisted these interceptions without Plaintiff's knowledge, consent, or express written authorization.

26. By failing to receive the requisite consent, Policygenius breached confidentiality and unlawfully disclosed Plaintiff's personal, private, and personally identifiable information and protected health information.

Defendant

27. Defendant Policygenius LLC is a Delaware entity with its principal place of business at 32 Old Slip, 30th Floor, New York City, New York 10005. Through Policygenius's Website, consumers are able to search for life, home, auto, and disability insurance policies. Defendant targets and solicits consumers in California and nationwide to apply to for insurance and is licensed by the California Department of Insurance. On information and belief, thousands of California residents use the Website each week.

COMMON FACTUAL ALLEGATIONS

Background: Underlying Technology Employed by Defendant for the Purpose of Disclosing Plaintiff and Class Members' Private Information to Facebook.

28. Defendant purposely installed the Pixel and Conversions API tools on many of its webpages within its Website and programmed those webpages to surreptitiously share its users' private and protected communications with Facebook, including communications that contain Plaintiff's and Class Members' PHI and PII.

29. Defendant uses the Website to connect Plaintiff and Class Members to

Defendant's digital insurance platforms with the goal of increasing profitability.

30. In order to understand Defendant's unlawful data-sharing practices, it is important first to understand basic web design and tracking tools.

Facebook's Business Tools and the Pixel

31. Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[6]

32. In conjunction with its advertising business, Facebook encourages and promotes entities and website owners, such as Defendant, to utilizes its "Business Tools" to gather, identify, target, and market products and services to individuals.

33. Facebook's Business Tools, including the Pixel and Conversions API, are bits of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of user activity on those platforms.

34. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, that webpage's Universal Resource Locator ("URL") and metadata, button clicks, etc.[7] Advertisers, such as

[6] FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Nov. 14, 2022)

[7] FACEBOOK, SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142. (last visited Nov. 14, 2022); *see* FACEBOOK, FACEBOOK PIXEL, ACCURATE EVENT

Defendant, can track other user actions and can create their own tracking parameters by building a "custom event."[8]

35. One such Business Tool is the Pixel which "tracks the people and type of actions they take."[9] When a user accesses a webpage that is hosting the Pixel, their communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook's servers—traveling from the user's browser to Facebook's server.

36. Notably, this transmission only occurs on webpages that contain the Pixel. Thus, Plaintiff's and Class Members' Private Information would not have been disclosed to Facebook via the Pixel but for Defendant's decisions to install the Pixel on its Website.

37. Similarly, Plaintiff's and Class Members' Private Information would not have been disclosed to Facebook via Conversions API but for Defendant's decision to install and implement that tool.

38. By installing and implementing both tools, Defendant caused Plaintiff's and Class Members' communications to be intercepted and transmitted to Facebook via the

TRACKING, ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* FACEBOOK, BEST PRACTICES FOR FACEBOOK PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Nov. 14, 2022).

[8] FACEBOOK, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/. (last visited Nov. 14, 2022)

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

Pixel, and it caused a second improper disclosure of that information via Conversions API.

39. As explained below, these unlawful transmissions are initiated by Defendant's source code concurrent with communications made via certain webpages.

Defendant's method of transmitting Plaintiff's and Class Members' Private Information via the Tracking Pixel and/or Conversions API i.e., the interplay between HTTP Requests and Responses, Source Code, and the Pixel

40. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the internet. Each "client device" (such as computer, tablet, or smart phone) accesses web content through a web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

41. Every website is hosted by a computer "server" that holds the website's contents and through which the entity in charge of the website exchanges communications with Internet users' devices via their web browsers.

42. Web communications consist of HTTP or HTTPS Requests and HTTP or HTTPS Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies:

- **HTTP Request**: an electronic communication sent from the user device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies. POST Requests can send a large amount of data outside of the URL. (For instance, uploading a PDF for filing a motion to a court)

- **Cookies**: a small text file that can be used to store information on the user device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from user devices to the host server. Some cookies are "third-party cookies," which means they can store and communicate data when visiting one website to an entirely different website.
- **HTTP Response**: an electronic communication that is sent as a reply to the user device's web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.[10]

43. A user's HTTP Request essentially asks the Defendant's Website to retrieve certain information (such as the "Home-owners insurance" page). The HTTP Response sends the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons, and other features that appear on the user's screen as they navigate Defendant's Website.

44. Every website is comprised of Markup and "Source Code." Source Code is simply a set of instructions that commands the website visitor's browser to take certain

[10] One browsing session may consist of hundreds or thousands of individual HTTP Requests and HTTP Responses.

actions when the web page first loads or when a specified event triggers the code.

45. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user. Defendant's Pixel is source code that does just that. The Pixel acts much like a traditional wiretap. When users visit Defendant's website via an HTTP Request to Policygenius's server, Defendant's server sends an HTTP Response including the Markup that displays the Webpage visible to the user and Source Code including Defendant's Pixel. Thus, Defendant is in essence handing users a tapped phone, and once the Webpage is loaded into the user's browser, the software-based wiretap is quietly waiting for private communications on the Webpage to trigger the tap, which intercepts those communications intended only for Defendant and transmits those communications to third-parties, including Facebook and Google.

46. Third parties, like Facebook, place third-party cookies in the web browsers of users logged into their services. These cookies uniquely identify the user and are sent with each intercepted communication to ensure the third-party can uniquely identify the user associated with the Personal Information intercepted.

47. With substantial work and technical know-how, internet users can sometimes circumvent this browser-based wiretap technology. This is why third parties bent on gathering Personal Information, like Facebook, implement workarounds that savvy users cannot evade. Facebook's workaround, for example, is called Conversions API.

Conversions API is an effective workaround because it does the transmission from their own servers and does not rely on the User's web browsers. Conversions API "is designed to create a direct connection between [Web hosts'] marketing data and [Facebook]." Thus, the communications between users and Defendant, which are necessary to use Defendant's Website, are actually received by Defendant and stored on its server before Conversions API collects and sends the Private Information contained in those communications directly from Defendant to Facebook. User devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.

48. While there is no way to confirm with certainty that a Web host like Defendant has implemented workarounds like Conversions API without access to the host server, companies like Facebook instruct Defendant to "[u]se the Conversions API in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows Defendant "to share website events [with Facebook] that the pixel may lose."[11] Thus, it is reasonable to infer that Facebook's customers who implement the Facebook Pixel in accordance with Facebook's documentation will also implement the Conversions API workaround.

49. The third parties to whom a website transmits data through pixels and associated workarounds do not provide any substantive content relating to the user's

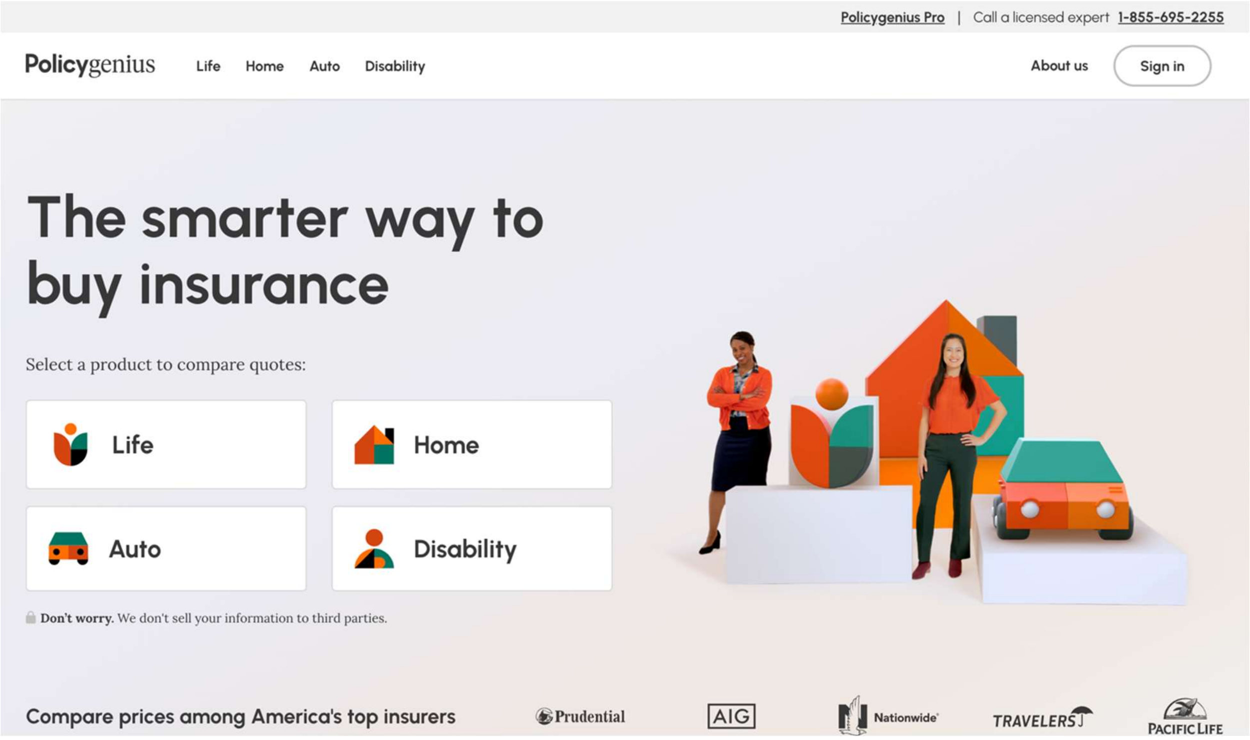
[11] *See* https://www.facebook.com/business/help/308855623839366?id=818859032317965 (last visited Jan. 23, 2023).

communications. Instead, these third parties are typically procured to track user data and communications for marketing purposes of the website owner (*i.e.,* to bolster profits).

50. Thus, without any knowledge, authorization, or action by a user, a website owner like Defendant can use its source code to commandeer the user's computing device, causing the device to contemporaneously and invisibly re-direct the users' communications to third parties.

51. In this case, Defendant employed the Tracking Pixel and Conversions API to intercept, duplicate, and re-direct Plaintiff's and Class Members' Private Information to Facebook.

52. For example, when a user visits www.policygenius.com and selects the "Home" button under the "Compare quotes" banner, the user's browser automatically sends an HTTP Request to Defendant's web server. Defendant's web server automatically returns an HTTP Response, which loads the Markup for that particular webpage. As depicted below, the user only sees the Markup, not Defendant's Source Code or underlying HTTP Requests and Responses.



The smarter way to buy insurance

Select a product to compare quotes:

Don't worry. We don't sell your information to third parties.

Compare prices among America's top insurers

Figure 1. The image above is a screenshot taken from the user's web browser upon visiting www.policygenius.com *(last accessed November 20, 2023).*

53. The Pixel is embedded in Defendant's Source Code contained in its HTTP Response. The Pixel, programmed to automatically track and transmit the user's communications with Defendant's Website to Facebook, executes instructions that effectively open a hidden spying window into the user's browser through which Facebook can intercept the visitor's data, actions, and communications with Defendant.[12]

[12] When used in the context of a screen or visual display, a "pixel" is the smallest unit in such a digital display. An image or video on a device's screen can be made up of millions of individual pixels. The Facebook Pixel is a tiny image file that is so small as to be invisible to website users. It is purposefully designed and camouflaged in this manner so that website users remain unaware of it.

54. Defendant's Source Code manipulates the user's browser by secretly instructing it to duplicate the user's communications (HTTP Requests) with Defendant and to send those communications to Facebook. These transmissions occur contemporaneously, invisibly, and without the user's knowledge.

55. Thus, without its users' consent, Defendant has effectively used its source code to commandeer and "bug" or "tap" its users' computing devices, allowing Facebook and other third parties to listen in on all of their communications with Defendant and thereby intercept those communications, including Private Information.

56. Consequently, when Plaintiff and Class Members visit Defendant's website and communicate their Private Information, including, but not limited to, button clicks and page visits are transmitted to third parties.

Defendant Disclosed Plaintiff's and Class Members' Private Information to Facebook Using the Pixel and/or Conversions API Tracking Practices

57. Defendant utilizes Facebook's Business Tools and intentionally installed the Pixel and Conversions API ("First Party cookies") on its Website and servers to secretly track users by recording their activity and experiences in violation of its common law, contractual, statutory, and regulatory duties and obligations.[13]

[13] *Id.*

58. Defendant's Pixel has its own unique identifier (represented as id=682897698520376), which can be used to identify which of Defendant's webpages contain the Pixel.

59. The Pixel allows Defendant to optimize the delivery of ads, measure cross-device conversions, create custom audiences, and decrease advertising and marketing costs.[14] However, Defendant's Website does not rely on the Pixel in order to function.

60. While seeking and using Defendant's services as an insurance provider, Plaintiff and Class Members communicated their Private Information to Defendant via its Website.

61. Plaintiff and Class Members were not aware that their Private Information would be shared with Facebook as it was communicated to Defendant because, amongst other things, Defendant did not disclose this fact.

62. Plaintiff and Class Members never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information to Facebook, nor did they intend for Facebook to be a party to their communications (many of them highly sensitive and confidential) with Defendant.

63. Defendant's Pixel and First Party cookies sent non-public Private Information to Facebook, including but not limited to Plaintiff's and Class Members': (1) desired insurance coverage; (2) zip code; (3) residential address and status; and (4) policy status.

[14] *Id.*

64. Importantly, the Private Information Defendant's Pixel sent to Facebook was sent alongside the Plaintiff's and Class Members' Facebook ID (c_user cookie or "FID"), thereby allowing individual users' communications with Defendant, and the Private Information contained in those communications, to be linked to their unique Facebook accounts and therefore their identity.[15]

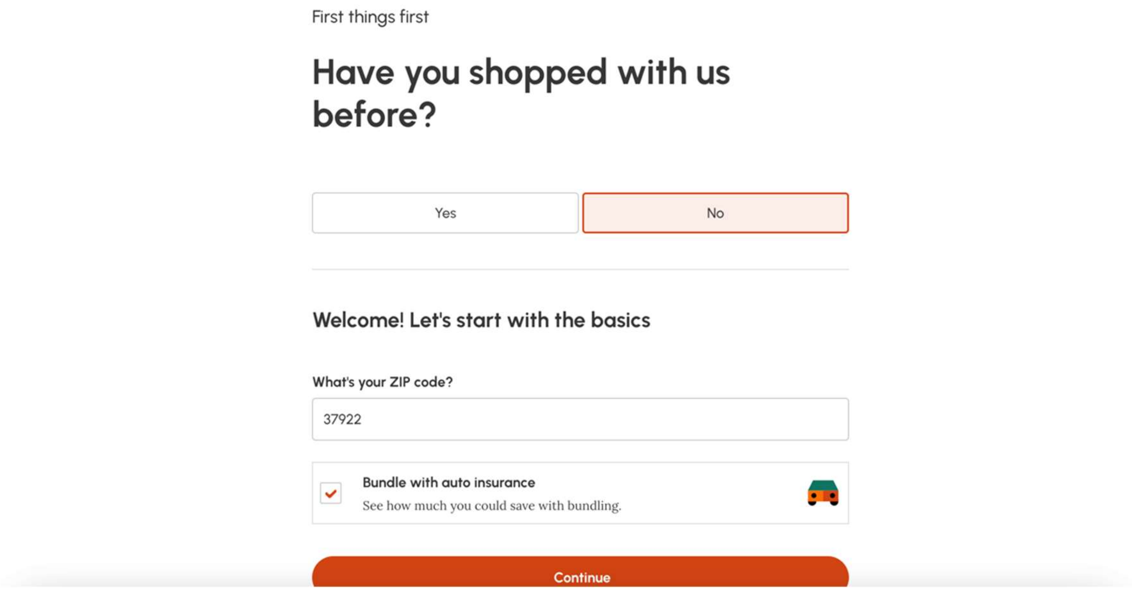
65. A user's FID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including location, pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook ID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the Facebook ID to locate, access, and view the user's corresponding Facebook profile quickly and easily.

66. Defendant deprived Plaintiff and Class Members of their privacy rights when it: (1) implemented technology (i.e., the Facebook Pixel and First Party cookies) that surreptitiously tracked, recorded, and disclosed Plaintiff's and other online users' confidential communications and Private Information; (2) disclosed users' protected information to Facebook—an unauthorized third-party; and (3) undertook this pattern of conduct without notifying Plaintiff or Class Members and without obtaining their express written consent.

[15] Defendant's Website track and transmit data via first-party and third-party cookies. The c_user cookie or FID is a type of third-party cookie assigned to each person who has a Facebook account, and it is comprised by a unique and persistent set of numbers.

Defendant's Pixel Disseminates User Information via Its Website

67. An example illustrates the point. If a user uses the Website to find home insurance, Defendant's Website directs them to communicate Private Information, including their zip code, and whether they own, rent, or are closing in the property they are insuring. Unbeknownst to the patient, each and every communication is sent to Facebook via Defendant's Pixel.


First things first

Have you shopped with us before?

Welcome! Let's start with the basics

What's your ZIP code?

37922

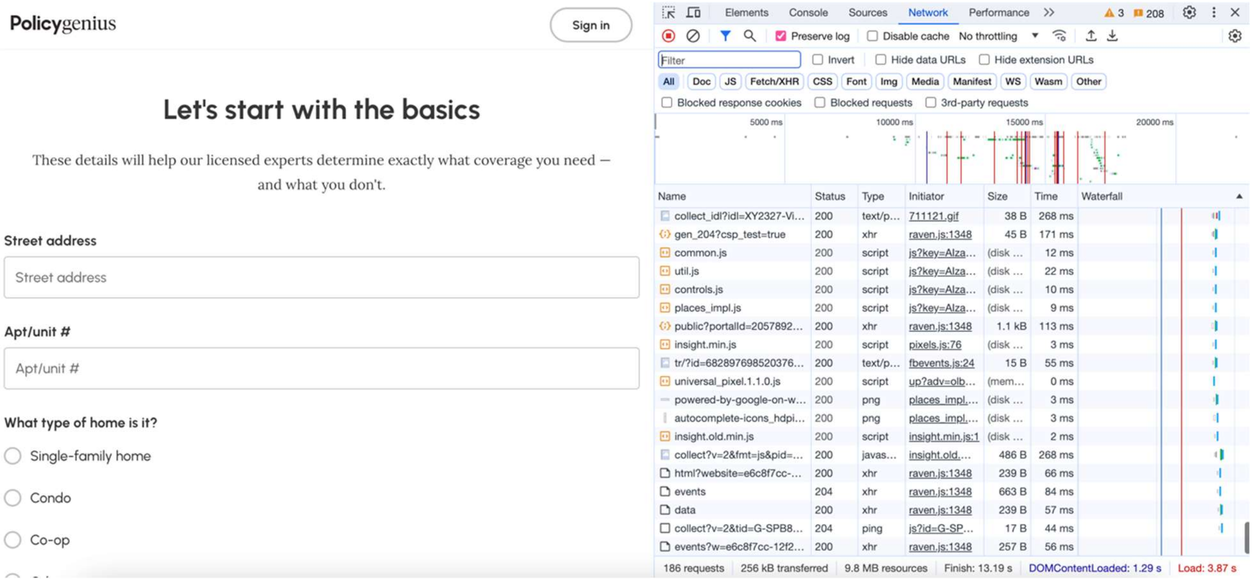
☑ Bundle with auto insurance
See how much you could save with bundling.

68. In the example above, the user is required to insert their home zip code before being allowed to move onto the next page.

69. Next, the user is required to provide the status of the ownership of the property they are seeking to insure, as well as their current home insurance agency and the length of their policy. Additionally, users are required to submit the address of the property they

are seeking to ensure, the type of home it is, specify if it is the user's primary residence, the length of residency there, and the mortgage rate of the home.

70. Unbeknownst to ordinary users, this particular webpage—which is undoubtedly used to communicate Private Information for the purpose of seeking insurance—contains Defendant's Pixel. The image below shows the "behind the scenes" portion of the website that is invisible to ordinary users. Importantly, each entry in the column represents just one instance in which Defendant's Pixel sent this particular user's information to Facebook.



Let's start with the basics

These details will help our licensed experts determine exactly what coverage you need – and what you don't.

Street address

Street address

Apt/unit #

Apt/unit #

What type of home is it?

○ Single-family home

○ Condo

○ Co-op

☑ Preserve log □ Disable cache No throttling

□ Invert □ Hide data URLs □ Hide extension URLs

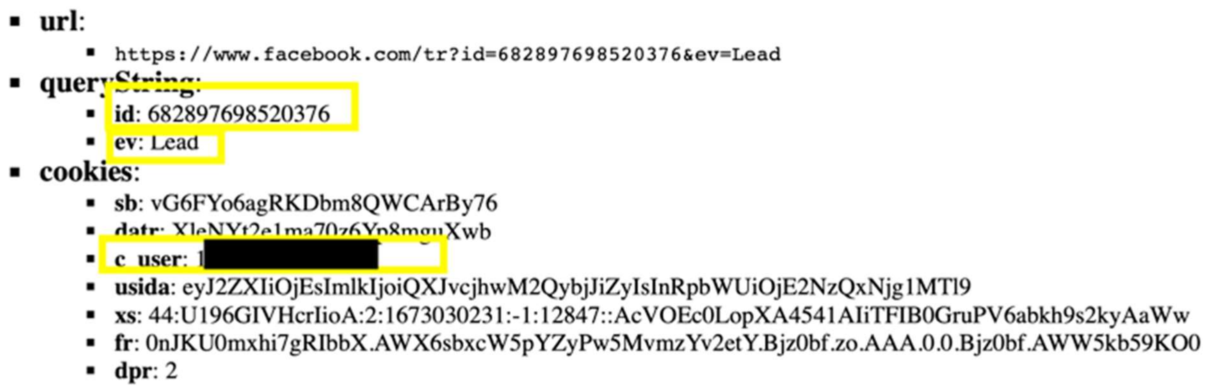
□ Blocked response cookies □ Blocked requests □ 3rd-party requests

Name	Status	Type	Initiator	Size	Time	Waterfall
collect_idl?idl=XY2327-Vi...	200	text/p...	711121.gif	38 B	268 ms	
gen_204?csp_test=true	200	xhr	raven.js:1348	45 B	171 ms	
common.js	200	script	js?key=Alza...	(disk ...	12 ms	
util.js	200	script	js?key=Alza...	(disk ...	22 ms	
controls.js	200	script	js?key=Alza...	(disk ...	10 ms	
places_impl.js	200	script	js?key=Alza...	(disk ...	9 ms	
public?portalId=2057892...	200	xhr	raven.js:1348	1.1 kB	113 ms	
insight.min.js	200	script	pixels.js:76	(disk ...	3 ms	
tr/?id=682897698520376...	200	text/p...	fbevents.js:24	15 B	55 ms	
universal_pixel.1.1.0.js	200	script	up?adv=olb...	(mem...	0 ms	
powered-by-google-on-w...	200	png	places_impl....	(disk ...	3 ms	
autocomplete-icons_hdpi...	200	png	places_impl....	(disk ...	3 ms	
insight.old.min.js	200	script	insight.min.js:1	(disk ...	2 ms	
collect?v=2&fmt=js&pid=...	200	javas...	insight.old....	486 B	268 ms	
html?website=e6c8f7cc-...	200	xhr	raven.js:1348	239 B	66 ms	
events	204	xhr	raven.js:1348	663 B	84 ms	
data	200	xhr	raven.js:1348	239 B	57 ms	
collect?v=2&tid=G-SPB8...	204	ping	js?id=G-SP...	17 B	44 ms	
events?w=e6c8f7cc-12f2...	200	xhr	raven.js:1348	257 B	56 ms	

186 requests | 256 kB transferred | 9.8 MB resources | Finish: 13.19 s | DOMContentLoaded: 1.29 s | Load: 3.87 s

71. Thus, without alerting the user, Defendant's Pixel sends each and every communication the user made via the webpage to Facebook, and the images below confirm

that the communications Defendant sends to Facebook contain the user's Private Information.



- **url**:
  - `https://www.facebook.com/tr?id=682897698520376&ev=Lead`
- **queryString**:
  - **id**: 682897698520376
  - **ev**: Lead
- **cookies**:
  - **sb**: vG6FYo6agRKDbm8QWCArBy76
  - **datr**: XleNYt2e1ma70z6Yp8mguXwb
  - **c_user**: [redacted]
  - **usida**: eyJ2ZXIiOjEsImlkIjoiQXJvcjhwM2QybjJiZyIsInRpbWUiOjE2NzQxNjg1MTl9
  - **xs**: 44:U196GIVHcrIioA:2:1673030231:-1:12847::AcVOEc0LopXA4541AIiTFIB0GruPV6abkh9s2kyAaWw
  - **fr**: 0nJKU0mxhi7gRIbbX.AWX6sbxcW5pYZyPw5MvmzYv2etY.Bjz0bf.zo.AAA.0.0.Bjz0bf.AWW5kb59KO0
  - **dpr**: 2

72. The first line of highlighted text, "id:682897698520376" refers to Defendant's Pixel ID and confirms that Defendant has downloaded the Pixel into its Source Code for this particular webpage.

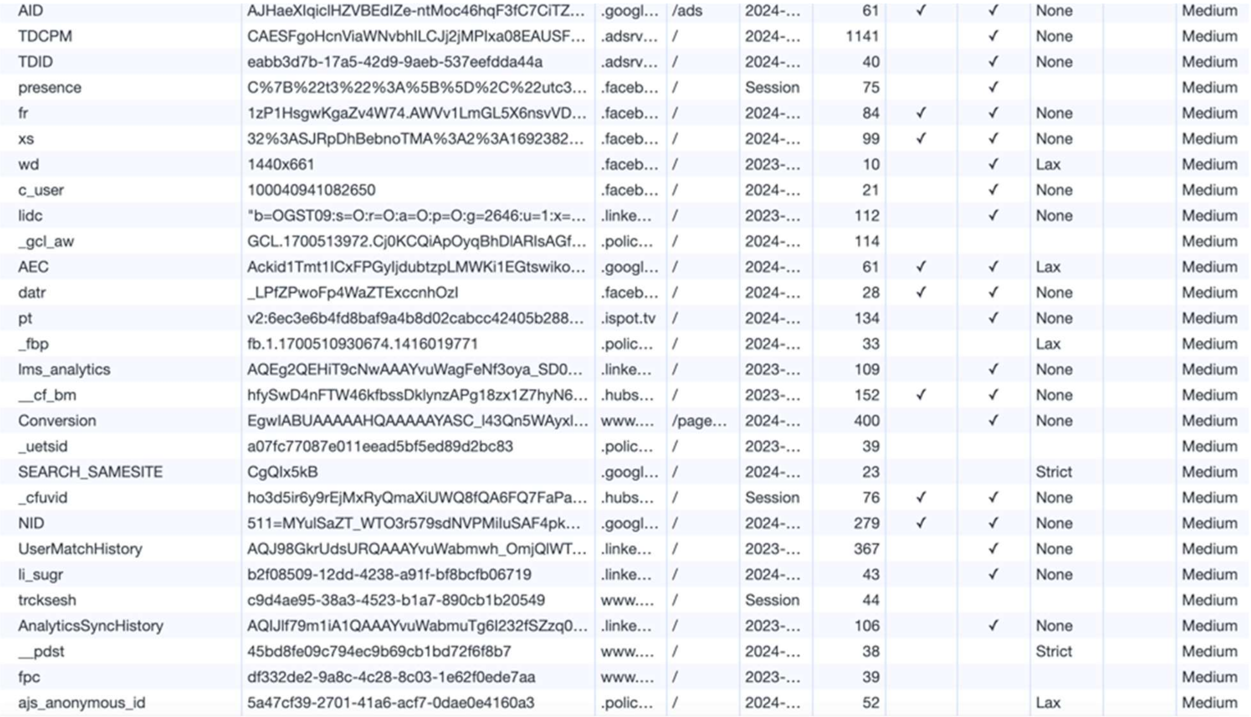
73. On the same line of text, "ev= Lead," identifies and categorizes which actions the user took on the webpage ("ev=" is an abbreviation for event, and "Lead" is the type of event). Thus, this identifies the user as having used the website in the URL.

74. Finally, the highlighted text c_user demonstrates that Defendant's Pixel sent the user's communications, and the Private Information contained therein, alongside the user's Facebook ID , thereby allowing the user's communications and actions on the website to be linked to their specific Facebook profile.

75. In each of the examples above, the user's website activity and the contents of the user's communications are sent to Facebook alongside their personally identifiable

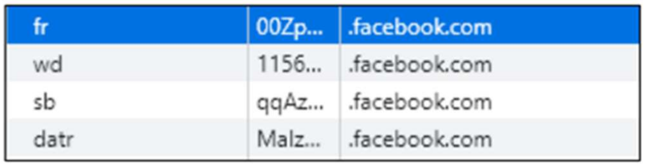
information. Several different methods allow marketers and third parties to identify individual website users, but the examples above demonstrate what happens when the website user is logged into Facebook on their web browser or device. When this happens, the website user's identity is revealed via third-party cookies that work in conjunction with the Pixel. For example, the Pixel transmits the user's c_user cookie, which contains that user's unencrypted Facebook ID, and allows Facebook to link the user's online communications and interactions to their individual Facebook profile.

76. Facebook receives at least six cookies when Defendant's website transmits information via the Pixel**:**



AID	AJHaeXlqiclHZVBEdlZe-ntMoc46hqF3fC7CiTZ...	.googl...	/ads	2024-...	61	✓	✓	None		Medium
TDCPM	CAESFgoHcnViaWNvbhILCJj2jMPIxa08EAUSF...	.adsrv...	/	2024-...	1141		✓	None		Medium
TDID	eabb3d7b-17a5-42d9-9aeb-537eefdda44a	.adsrv...	/	2024-...	40		✓	None		Medium
presence	C%7B%22t3%22%3A%5B%5D%2C%22utc3...	.faceb...	/	Session	75		✓			Medium
fr	1zP1HsgwKgaZv4W74.AWVv1LmGL5X6nsvVD...	.faceb...	/	2024-...	84	✓	✓	None		Medium
xs	32%3ASJRpDhBebnoTMA%3A2%3A1692382...	.faceb...	/	2024-...	99	✓	✓	None		Medium
wd	1440x661	.faceb...	/	2023-...	10		✓	Lax		Medium
c_user	100040941082650	.faceb...	/	2024-...	21		✓	None		Medium
lidc	"b=OGST09:s=O:r=O:a=O:p=O:g=2646:u=1:x=...	.linke...	/	2023-...	112		✓	None		Medium
_gcl_aw	GCL.1700513972.Cj0KCQiApOyqBhDIARIsAGf...	.polic...	/	2024-...	114					Medium
AEC	Ackid1Tmt1ICxFPGyljdubtzpLMWKi1EGtswiko...	.googl...	/	2024-...	61	✓	✓	Lax		Medium
datr	_LPfZPwoFp4WaZTExccnhOzl	.faceb...	/	2024-...	28	✓	✓	None		Medium
pt	v2:6ec3e6b4fd8baf9a4b8d02cabcc42405b288...	.ispot.tv	/	2024-...	134		✓	None		Medium
_fbp	fb.1.1700510930674.1416019771	.polic...	/	2024-...	33			Lax		Medium
lms_analytics	AQEg2QEHiT9cNwAAAYvuWagFeNf3oya_SD0...	.linke...	/	2023-...	109		✓	None		Medium
__cf_bm	hfySwD4nFTW46kfbssDklynzAPg18zx1Z7hyN6...	.hubs...	/	2023-...	152	✓	✓	None		Medium
Conversion	EgwIABUAAAAAHQAAAAAYASC_l43Qn5WAyxl...	www....	/page...	2024-...	400		✓	None		Medium
_uetsid	a07fc77087e011eead5bf5ed89d2bc83	.polic...	/	2023-...	39					Medium
SEARCH_SAMESITE	CgQIx5kB	.googl...	/	2024-...	23			Strict		Medium
_cfuvid	ho3d5ir6y9rEjMxRyQmaXiUWQ8fQA6FQ7FaPa...	.hubs...	/	Session	76	✓	✓	None		Medium
NID	511=MYulSaZT_WTO3r579sdNVPMiluSAF4pk...	.googl...	/	2024-...	279	✓	✓	None		Medium
UserMatchHistory	AQJ98GkrUdsURQAAAYvuWabmwh_OmjQlWT...	.linke...	/	2023-...	367		✓	None		Medium
li_sugr	b2f08509-12dd-4238-a91f-bf8bcfb06719	.linke...	/	2024-...	43		✓	None		Medium
trcksesh	c9d4ae95-38a3-4523-b1a7-890cb1b20549	www....	/	Session	44					Medium
AnalyticsSyncHistory	AQIJIf79m1iA1QAAAYvuWabmuTg6I232fSZzq0...	.linke...	/	2023-...	106		✓	None		Medium
__pdst	45bd8fe09c794ec9b69cb1bd72f6f8b7	www....	/	2024-...	38			Strict		Medium
fpc	df332de2-9a8c-4c28-8c03-1e62f0ede7aa	www....	/	2023-...	39					Medium
ajs_anonymous_id	5a47cf39-2701-41a6-acf7-0dae0e4160a3	.polic...	/	2024-...	52			Lax		Medium

77. When a visitor's browser has recently logged out of an account, Facebook compels the visitor's browser to send a smaller set of cookies:[16]



fr	00Zp...	.facebook.com
wd	1156...	.facebook.com
sb	qqAz...	.facebook.com
datr	Malz...	.facebook.com

78. The fr cookie contains an encrypted Facebook ID and browser identifier.[17] Facebook, at a minimum, uses the fr cookie to identify users, and this particular cookie can stay on a user's website browser for up to 90 days after the user has logged out of Facebook.[18]

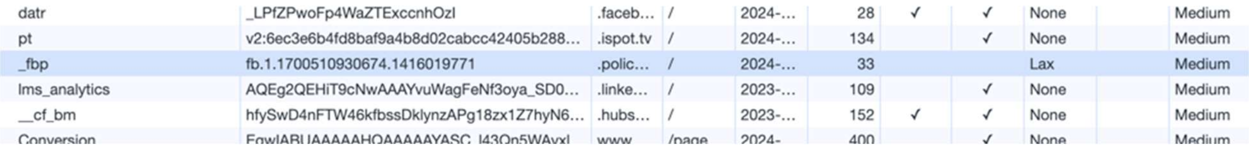
79. The cookies listed in the two images above are commonly referred to as third-party cookies because they were "created by a website with a domain name other than the one the user is currently visiting"—i.e., Facebook. Although Facebook created these cookies, Defendant is ultimately responsible for the manner in which individual website users were identified via these cookies, and Facebook would not have received this data but for Defendant's implementation and use of the Pixel throughout its website.

[16] The screenshot below serves as example and demonstrates the types of data transmitted during an HTTP single communication session. Not pictured here and in the preceding image is the _fbp cookie, which is transmitted as a first-party cookie.

[17] Data Protection Commissioner, Facebook Ireland Ltd: Report of Re-Audit (Sept. 21, 2012), p. 33, http://www.europe-v-facebook.org/ODPC_Review.pdf (last visited May 11, 2023).

[18] Cookies & other storage technologies, FACEBOOK.COM, https://www.facebook.com/policy/cookies/ (last visited May 11, 2023).

80. Defendant also revealed its website visitors' identities via first-party cookies such as the _fbp cookie that Facebook uses to identify a particular browser and a user:[19]



datr	_LPfZPwoFp4WaZTExccnhOzl	.faceb...	/	2024-...	28	✓	✓	None		Medium
pt	v2:6ec3e6b4fd8baf9a4b8d02cabcc42405b288...	.ispot.tv	/	2024-...	134		✓	None		Medium
_fbp	fb.1.1700510930674.1416019771	.polic...	/	2024-...	33			Lax		Medium
lms_analytics	AQEg2QEHiT9cNwAAAYvuWagFeNf3oya_SD0...	.linke...	/	2023-...	109		✓	None		Medium
__cf_bm	hfySwD4nFTW46kfbssDklynzAPg18zx1Z7hyN6...	.hubs...	/	2023-...	152	✓	✓	None		Medium
Conversion	FgwIABUAAAAAHQAAAAAYASC_I43Qn5WAvxI	www	/page	2024-	400		✓	None		Medium

81. Importantly, the _fbp cookie is transmitted to Facebook even when the user's browser is configured to block third-party tracking cookies because, unlike the fr cookies and c_user cookie, the _fbp cookie functions as a first-party cookie—i.e. a cookie that was created and placed on the website by Defendant.[20]

82. The Facebook Tracking Pixel uses both first- and third-party cookies.

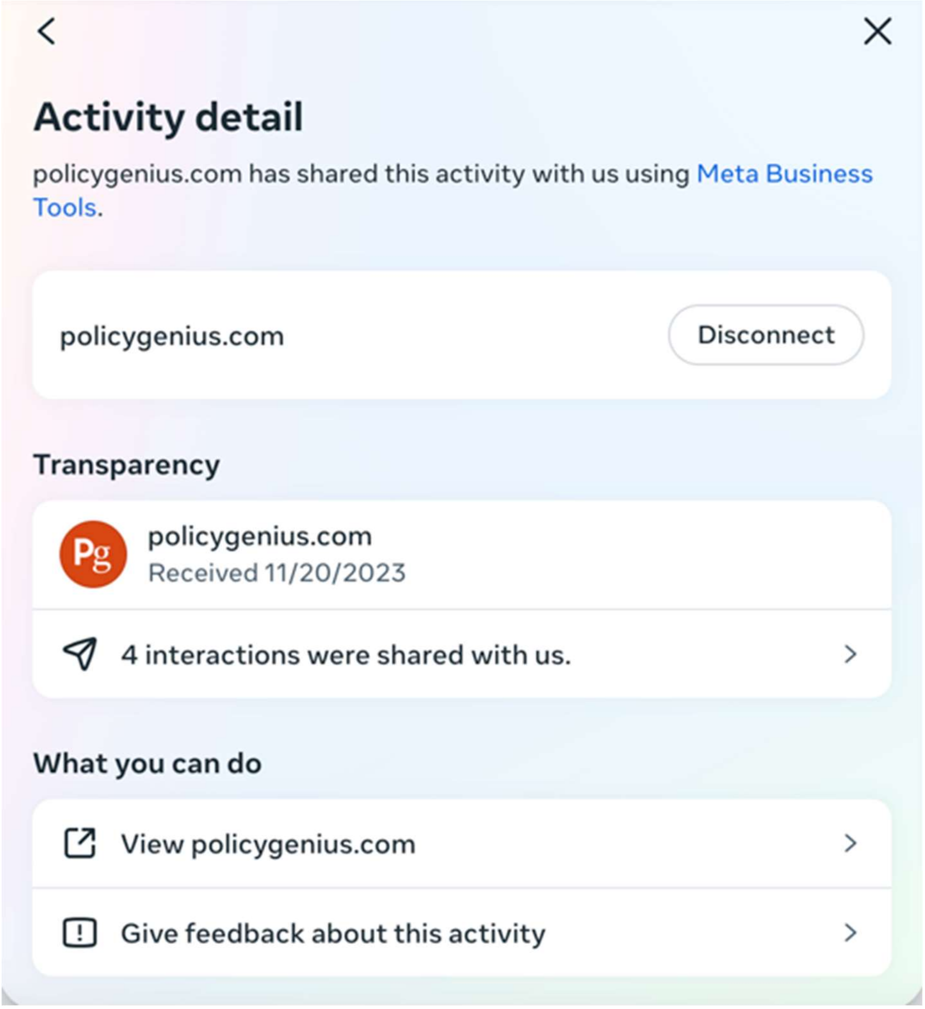
83. In summation, Facebook, at a minimum, uses the fr, _fbp, and c_user cookies to link website visitors' communications and online activity with their corresponding Facebook profiles, and, because the Pixel is automatically programmed to transmit data via both first-party and third-party cookies, users' information and identities are revealed to Facebook even when they have disabled third-party cookies within their web browsers.

84. The image below, gathered from a website visitor's own Facebook account after the fact, makes it patently clear that Defendant is actively sending patient

[19] *Id.*

[20] The _fbp cookie is always transmitted as a first-party cookie. A duplicate _fbp cookie is sometimes sent as a third-party cookie, depending on whether the browser has recently logged into Facebook.

communications to Facebook, stating Policygenius shared the user's information four times using Facebook business tools.



Activity detail

policygenius.com has shared this activity with us using Meta Business Tools.

policygenius.com Disconnect

Transparency

policygenius.com
Received 11/20/2023

4 interactions were shared with us.

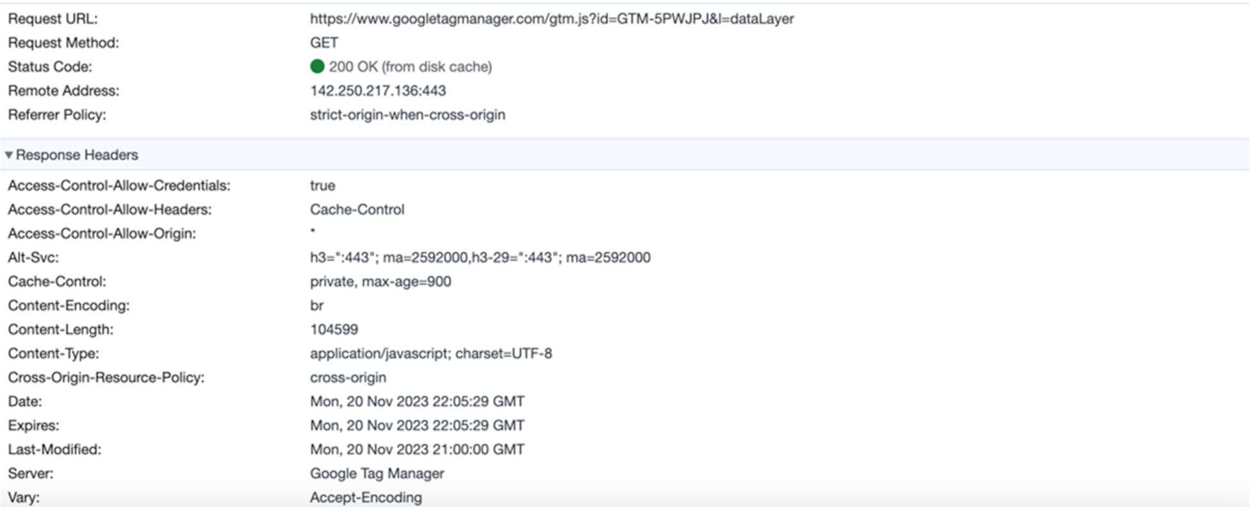
What you can do

View policygenius.com

Give feedback about this activity

85. At present, the full breadth of Defendant's tracking and data sharing practices is unclear, but other evidence suggests Defendant is using additional tracking pixels and tools to transmit its users' Private Information to additional third parties. For example, the image below indicates that Defendant is also sending its users' protected health information to Google via Google Tag Manager.

86. The image below contains the URL the user visited was sent to Google, and Defendant does not appear to have enabled the anonymize feature provided by Google because the text "aip:" does not appear in the image.



```
Request URL:                         https://www.googletagmanager.com/gtm.js?id=GTM-5PWJPJ&l=dataLayer
Request Method:                      GET
Status Code:                         ● 200 OK (from disk cache)
Remote Address:                      142.250.217.136:443
Referrer Policy:                     strict-origin-when-cross-origin
▾ Response Headers
Access-Control-Allow-Credentials:    true
Access-Control-Allow-Headers:        Cache-Control
Access-Control-Allow-Origin:         *
Alt-Svc:                             h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control:                       private, max-age=900
Content-Encoding:                    br
Content-Length:                      104599
Content-Type:                        application/javascript; charset=UTF-8
Cross-Origin-Resource-Policy:        cross-origin
Date:                                Mon, 20 Nov 2023 22:05:29 GMT
Expires:                             Mon, 20 Nov 2023 22:05:29 GMT
Last-Modified:                       Mon, 20 Nov 2023 21:00:00 GMT
Server:                              Google Tag Manager
Vary:                                Accept-Encoding
```

87. Accordingly, Google receives users' communications alongside the users' IP address, which is also impermissible under HIPAA.

88. Defendant does not disclose that the Pixel, First Party cookies, Google Tag Manager, or any other tracking tools embedded in the Website's source code tracks, records, and transmits Plaintiff's and Class Members' Private Information to Facebook and Google. Moreover, Defendant never received consent or written authorization to disclose Plaintiff's and Class Members' private communications to Facebook or Google

A. Facebook Exploited and Used Plaintiff's and Class Members' Private Information

89. Unsurprisingly, Facebook does not offer its Pixel to companies like Defendant solely for Defendant's benefit. "Data is the new oil of the digital economy,"[21] and Facebook has built its more-than $300 billion market capitalization on mining and using that "digital" oil. Thus, the large volumes of personal and sensitive health-related data Defendant provides to Facebook are actively examined, curated, and put to use by the company. Facebook acquires the raw data to transform it into a monetizable commodity, just as an oil company acquires crude oil to transform it into gasoline. Indeed, Facebook offers the Pixel free of charge[22] and the price that Defendant pays for the pixel is the data that it allows Facebook to collect.

90. Facebook describes itself as a "real identity platform,"[23] meaning users are allowed only one account and must share "the name they go by in everyday life."[24] To that end, when creating an account, users must provide their first and last name, date of birth, and gender.[25]

[21] https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/ (last visited November 27, 2023).

[22] https://seodigitalgroup.com/facebook-pixel/ (last visited November 27, 2023).

[23] Sam Schechner and Jeff Horwitz, *How Many Users Does Facebook Have? The Company Struggles to Figure It Out*, WALL. ST. J. (Oct. 21, 2021).

[24] FACEBOOK, COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY, https://www.facebook.com/communitystandards/integrity_authenticity (last visited November 27, 2023).

[25] FACEBOOK, SIGN UP, https://www.facebook.com/ (last visited November 27, 2023).

91. Facebook sells advertising space by emphasizing its ability to target users.[26] Facebook is especially effective at targeting users because it surveils user activity both on and off its site (with the help of companies like Defendant).[27] This allows Facebook to make inferences about users beyond what they explicitly disclose, including their "interests," "behavior," and "connections."[28] Facebook compiles this information into a generalized dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.[29]

92. Advertisers can also build "Custom Audiences,"[30] which helps them 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."[31] With Custom

[26] FACEBOOK, WHY ADVERTISE ON FACEBOOK, https://www.facebook.com/business/help/205029060038706 (last visited November 27, 2023).

[27] FACEBOOK, ABOUT FACEBOOK PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited November 27, 2023).

[28] FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting (last visited November 27, 2023).

[29] FACEBOOK, EASIER, MORE EFFECTIVE WAYS TO REACH THE RIGHT PEOPLE ON FACEBOOK, https://www.facebook.com/business/news/Core-Audiences (last visited November 27, 2023).

[30] FACEBOOK, ABOUT CUSTOM AUDIENCES, https://www.facebook.com/business/help/744354708981227?id=2469097953376494 (last visited November 27, 2023).

[31] FACEBOOK, AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting (last visited November 27, 2023).

Audiences, advertisers can target existing customers directly, and they can also build "Lookalike Audiences," which "leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[32] Unlike Core Audiences, Custom Audiences and Lookalike Audiences are only available if the advertiser has sent its underlying data to Facebook. This data can be supplied to Facebook by manually uploading contact information for customers or by utilizing Facebook's "Business Tools."[33]

93. The Facebook Pixel, and the personal data mined and curated with it, is key to this business. 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."[34]

94. Facebook does not merely collect information gathered by the Pixel and store it for safekeeping on its servers without ever accessing the information. Instead, in accordance with the purpose of the Pixel to allow Facebook to create Core, Custom, and

[32] Facebook, About Lookalike Audiences, https://www.facebook.com/business/help/164749007013531?id=401668390442328 (last visited November 27, 2023).

[33] FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, https://www.facebook.com/business/help/170456843145568?id=2469097953376494 (last visited November 27, 2023).

[34] FACEBOOK, THE FACEBOOK BUSINESS TOOLS, https://www.facebook.com/help/331509497253087 (last visited November 27, 2023).

Lookalike Audiences for advertising and marketing purposes, Facebook viewed, processed, and analyzed Plaintiff's and Class Members' confidential Private Information. Upon information and belief, such viewing, processing, and analyzing was performed by computers and/or algorithms programmed and designed by Facebook employees at the direction and behest of Facebook.

95. Facebook receives over four petabytes of information every day and must rely on analytical tools designed to view, categorize, and extrapolate the data to augment human effort.[35] This process is known as data ingestion and allows "businesses to manage and make sense of large amounts of data."[36]

96. By using these tools, Facebook is able to rapidly translate the information it receives from the Pixel to display relevant ads to consumers. For example, if a consumer visits a retailer's webpage and places an item in their shopping cart without purchasing it, the next time the shopper visits Facebook, an ad for that item will appear on the shopper's Facebook page.[37] This evidences that Facebook views and categorizes data as they are received from the Pixel.

97. Moreover, even if Facebook eventually deletes or anonymizes sensitive information that it receives, it must first view that information to identify it as containing

[35] https://medium.com/@srank2000/how-facebook-handles-the-4-petabyte-of-data-generated-per-day-ab86877956f4 (last visited November 27, 2023).
[36] https://scaleyourapp.com/what-database-does-facebook-use-a-1000-feet-deep-dive/ (last visited November 27, 2023).
[37] https://www.oberlo.com/blog/facebook-pixel (last visited November 27, 2023).

sensitive information suitable for removal. Accordingly, there is a breach of confidentiality once the information is disclosed or received without authorization.

B. Defendant Was Enriched and Benefitted from the Use of The Pixel and Unauthorized Disclosures and Plaintiff's and Class Members' Data and Private Information Had Financial Value

98. The primary motivation and a determining factor in Defendant's interception and disclosure of Plaintiff's and Class Members' Private Information was to commit tortious acts as alleged herein; namely, the use of Private Information for advertising in the absence of express written consent. Defendant's further use of the Private Information after the initial interception and disclosure for marketing and revenue generation was an invasion of privacy.

99. In exchange for disclosing the Private Information of its users, Defendant is compensated by Facebook in the form of enhanced advertising services and more cost-efficient marketing on its platform.

100. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions. Upon information and belief, as part of its marketing campaign, Defendant re-targeted customers and potential customers.

101. Upon information and belief, Defendant was advertising its services on Facebook, and the Pixel was used to help Defendant understand the success of its advertisement efforts on Facebook. Defendant, in coordination with Facebook, associated

Plaintiff's and Class Members' Personal Information with preexisting Facebook user profiles.

102. By utilizing the Pixel, the cost of advertising and retargeting was reduced, thereby benefitting Defendant.

103. Defendant's disclosure of Private Information also hurt Plaintiff and the Class. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure will keep increasing, and estimates are as high as $434 per user, for a total of more than $200 billion industry wide.

104. The value of health data in particular is well-known and has been reported on extensively in the media. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry," in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[38]

105. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[39]

[38] *See* https://time.com/4588104/medical-data-industry/ (last visited November 27, 2023).
[39] *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited November 27, 2023).

106. Indeed, numerous marketing services and consultants offering advice to companies on how to build their email and mobile phone lists—including those seeking to take advantage of targeted marketing—direct putative advertisers to offer consumers something of value in exchange for their personal information. "No one is giving away their email address for free. Be prepared to offer a book, guide, webinar, course or something else valuable."[40]

107. There is also a market for data in which consumers can participate. Personal information has been recognized by courts as extremely valuable. *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig*., 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

108. Several companies have products through which they pay consumers for a license to track their data. Google, Nielsen, UpVoice, HoneyGain, and SavvyConnect are all companies that pay for browsing history information.

109. Meta itself has paid users for their digital information, including browsing history. Until 2019, Meta ran a "Facebook Research" app through which it paid $20 a

[40] Vero, How to Collect Emails Addresses on Twitter (June 2014), available at https://www.getvero.com/resources/twitter-lead-generation-cards/ (last visited November 27, 2023).

month for a license to collect browsing history information and other communications from consumers between the ages 13 and 35.

110. Additionally, healthcare data may be valued at up to $250 per record on the black market.[41]

TOLLING OF THE STATUTE OF LIMITATIONS & DELAYED DISCOVERY

111. All applicable statute(s) of limitations have been tolled by the delayed discovery doctrine. Plaintiff and Class Members could not have reasonably discovered Facebook's practice of tracking and intercepting their activities and communications on Defendant's website until this class action litigation commenced.

112. Plaintiff did not learn of Facebook's interception of their activities and communications on Defendant's website until being informed by the undersigned counsel of record before this complaint was filed.

113. Plaintiff had no reason to believe her Private Information was being intercepted through Defendant's website at all, let alone in real time while Plaintiff was inputting information into Defendant's website but before Plaintiff submitted her application. As detailed above, Defendant's privacy policy hyperlinks were buried on the bottom of Defendant's homepage, and Plaintiff was not presented with a conspicuous clickwrap listing the privacy policy hyperlinks. Furthermore, the technologies Defendant

[41] Tori Taylor, *Hackers, Breaches, and the Value of Healthcare Data, SecureLink* (June 30, 2021), https://www.securelink.com/blog/healthcare-data-new-prize-hackers (last visited November 27, 2023).

embedded on its website are not visible to the reasonable user—they are invisible and work in the background.

114. As a result, any and all applicable statutes of limitations otherwise applicable to the allegations herein have been tolled.

CLASS ACTION ALLEGATIONS

115. **Class Definition:** Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of herself and other similarly situated individuals defined as: all persons in California who, during the class period, provided their personally identifiable information and/or health information to Policygenius using www.policygenius.com (the "Class").

116. Plaintiff reserves the right to modify the class definitions or add sub-classes as necessary prior to filing a motion for class certification, at class certification, or at any later time as the Court permits.

117. 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.

118. Excluded from the Class is Policygenius; any affiliate, parent, or subsidiary of Policygenius; any entity in which Policygenius has a controlling interest; any officer director, or employee of Policygenius; any successor or assign of Policygenius; anyone

employed by counsel in this action; any judge to whom this case is assigned, his or her spouse and immediate family members; and members of the judge's staff.

119. Numerosity/Ascertainability. Members of the Class are so numerous that joinder of all members would be unfeasible and not practicable. The exact number of Class Members is unknown to Plaintiff at this time. However, it is estimated that there are thousands of individuals in the Class. The identity of such membership is readily ascertainable from Policygenius's records and non-parties' records.

120. Typicality. Plaintiff's claims are typical of the claims of the Class because Plaintiff used www.policygenius.com and had their Private Information disclosed to third parties without their express written authorization or knowledge. Plaintiff's claims are based on the same legal theories as the claims of other Class Members.

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

122. Common Questions of Law and Fact Predominate/Well Defined Community of Interest. Questions of law and fact common to the Class Members predominate over questions that may affect only individual Class Members because Defendant has acted on

grounds generally applicable to the Class. Such generally applicable conduct is inherent in Defendant's wrongful conduct. The following questions of law and fact are common to the Class:

a. Whether Plaintiff and Class Members had a reasonable expectation of privacy under the circumstances;

b. Whether Defendant's website surreptitiously records personally identifiable information, protected health information, financial information, and related communications and subsequently, or simultaneously, discloses that information to third parties;

c. Whether Defendant disseminated Class Members' confidential communications to third parties;

d. Whether Policygenius's conduct resulted in a breach of confidentiality;

e. Whether Policygenius violated Plaintiff's and Class Members' privacy rights by using software to record and communicate website visitor's personally identifiable information, including unique identifies and FIDs, alongside confidential medical communications;

f. Whether Plaintiff and Class Members are entitled to damages under CIPA, ECPA, or any other relevant statute;

g. Whether Defendant's actions violate Plaintiff's and Class Members' privacy rights as provided by the California Constitution; and

h. Whether Defendant's actions violated California's Unfair Competition Law, Bus. and Prof. Code § 17200 *et seq.* by, among other things, surreptitiously recording personally identifiable information, protected health information, financial information, and related communications and subsequently, or simultaneously, disclosing that information to third parties.

123. Superiority. Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit 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 a method for obtaining redress on claims that could not practicably be pursued individually, substantially outweighs potential difficulties in management of this class action. Plaintiff is unaware of any special difficulty to be encountered in litigating this action that would preclude its maintenance as a class action.

CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION
Violation Of the California Invasion of Privacy Act,
Cal. Penal Code § 630, *et seq*

124. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the proposed Class.

125. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630 to 638. The Act begins with its statement of purpose:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

Cal. Penal Code § 630.

126. California Penal Code § 631(a) provides, in pertinent part:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner … [ii] willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; [iii] or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or [iv] **who aids, agrees with, employs, or conspires** with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars ($2,500).

127. A defendant must show it had the consent of <u>all</u> parties to a communication.

128. Plaintiff's and Class Members' specific user input events and choices and information typed on Defendant's website are tracked by Defendant using the SDK provided by third parties, such as Facebook. The user's affirmative actions, such as

inputting information, selecting options, or relaying a response, and constitute communications within the scope of CIPA.

129. At all relevant times, Defendant aided, agreed with, and conspired with third parties, such as Facebook, to track and intercept Plaintiff's and Class Members' internet communications while accessing www.policygenius.com. These communications were intercepted without the authorization and consent of Plaintiff and Class Members.

130. Defendant intentionally inserted an electronic device into its website that, without the knowledge and consent of Plaintiff and Class Members, tracked and transmitted the substance of their confidential communications with Defendant to a third party.

131. Defendant willingly facilitated Facebook's interception and collection of Plaintiff's and Class Members' Private Information by embedding the Facebook Pixel on its website.

132. Defendant intended to share Plaintiff's and Class Members' private and personal information and communications to help the third parties learn some meaning of the content of the communications.

133. Plaintiff and Class Members are residents of California and used their devices within California. As such, Defendant records and disseminates Plaintiff's and Class Members' data, communications, and personal information in California.

134. Plaintiff and Class Members did not consent to any of Defendant's actions in implementing the tracking software. Nor have Plaintiff or Class Members consented to Defendant's intentional collection and sharing of Plaintiff's and Class Members' electronic communications, personally identifiable information, medical information, or financial information.

135. At all relevant times to this complaint, Plaintiff and the other Class Members did not know Defendant was engaging in such recording and sharing of information, and therefore could not provide consent to have any part of their private and confidential communications, personally identifiable information, financial information, and/or medical information intercepted and recorded by Defendant and thereafter transmitted to others.

136. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, the software in the source code of Policygenius's website, such as the Facebook Tracking Pixel, falls under the broad catch-all category of "any other manner":

a. The computer codes and programs third parties, such as Facebook, used to track Plaintiff's and Class Members' communications while they were navigating www.policygenius.com;

b. Plaintiff's and Class Members' browsers;

c. Plaintiff's and Class Members' computing and mobile devices;

d. Facebook's web and ad servers;

e. The web and ad-servers from which third parties, including Facebook, tracked and intercepted Plaintiff's and Class Members' communications while they were using a web browser to access or navigate www.policygenius.com; and

f. The computer codes and programs used by third parties, including Facebook, to effectuate its tracking and interception of Plaintiff's and Class Members' communications while they were using a browser to visit Defendant's website.

137. Defendant fails to disclose that it is using software from third parties, such as Facebook Pixel, specifically to track and automatically and simultaneously transmit communications, personally identifiable information, and protected health information to a third parties, *e.g.*, Facebook. Defendant is aware that these communications are confidential as its "Privacy Policy" acknowledges the confidential nature of private medical information but fails to disclose to website visitors who submit an insurance quote that Policygenius will record and provide their private and personal information with third parties.

138. The private information that Defendant transmits while using third party software, such as Facebook Pixel, including medical information consumers enter into the website, IP addresses, phone numbers and home addresses constitute confidential protected health information and personally identifiable information.

139. The Pixel is designed such that they transmit each of the users' actions taken on the webpage to a third party alongside and contemporaneously with the user initiating the communication. Thus, the communication is intercepted in transit to the intended recipient, Defendant and before it reaches Defendant's server.

140. As demonstrated hereinabove, Defendant violates CIPA by aiding and permitting third parties to receive its users' online communications through its website without their consent.

141. As a direct and proximate result of Defendant's violation of the CIPA, Plaintiff and Class Members were injured and suffered damages, a loss of privacy, and loss of the value of their personal information in an amount to be determined at trial.

142. By disclosing Plaintiff's and Class Members' Private Information, Defendant violated Plaintiff's and Class Members' statutorily protected right to privacy.

143. As a result of the above violations and pursuant to CIPA Section 637.2, Defendant is liable to each Plaintiff and Class Member for the greater of treble actual damages related to their loss of privacy in an amount to be determined at trial or for statutory damages in the amount of $5,000 per violation. Section 637.2 specifically states that "[it] is not a necessary prerequisite to an action pursuant to this section that the Plaintiff has suffered, or be threatened with, actual damages."

144. Under the statute, Defendant is also liable for reasonable attorney's fees, litigation costs, and injunctive and declaratory relief.

SECOND CAUSE OF ACTION
Invasion of Privacy Under California's Constitution

145. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

146. The California Constitution recognizes the right to privacy inherent in all residents of the State and creates a private right of action against private entities that invade that right.

147. Article I, Section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."

148. The right to privacy was added to the California Constitution in 1972, through Proposition 11 (called the "Right to Privacy Initiative"). Proposition 11 was designed to codify the right to privacy, protecting individuals from invasions of privacy from both the government and private entities alike:

> "The right of privacy is the right to be left alone. It is a fundamental and compelling interest. . . . It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulation of personal information."[42]

[42] Ballot Pamp., Proposed Stats. and Amends. to Cal. Const. with arguments to voters, Gen. Elec. (Nov. 7, 1972), argument in favor of Prop. 11, p. 27; *see also Hill v. Colorado*,530 U.S. 703, 716 (2000) (the right to privacy includes right to be free in one's

149. Plaintiff and Class Members have a legally protected privacy interests, as recognized by the California Constitution, CIPA, common law and the 4th Amendment to the United States Constitution.

150. Plaintiff and Class Members had a reasonable expectation of privacy under the circumstances, as they could not have reasonably expected that Defendant would violate state and federal privacy laws.

151. Plaintiff and Class Members were not aware and could not have reasonably expected that Policygenius would surreptitiously install software on its website to automatically track and transmit to third parties each Plaintiff's and Class Members' personally identifiable information, confidential communications and medical information.

152. Plaintiff and Class Members have an interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential communications and protected health information and financial 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 Plaintiff's and Class Members' knowledge or consent.

153. At all relevant times, by using software, such as Facebook's Tracking Pixel, to record and communicate Plaintiff's and Class Members' personally identifiable

home from unwanted communication); *Hill v. National Collegiate Athletic Assn.* (1994), 7 Cal.4th 1, 81, (Mosk, J., dissenting).

information, including unique identifiers and FIDs alongside their confidential communications and medical information, Policygenius intentionally invaded Plaintiff's and Class Members' privacy rights under the California Constitution.

154. Plaintiff and Class Members did not authorize Policygenius to record and transmit to third parties Plaintiff's and Class Members' private communications alongside their personally identifiable information and health information.

155. This invasion of privacy is serious in nature, scope, and impact because it relates to Plaintiff's and Class Members' private communications, personally identifiable information, and medical information. Moreover, it constitutes an egregious breach of the societal norms underlying the privacy right.

156. As a result of Defendant's actions, Plaintiff and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

157. Plaintiff and Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

158. Plaintiff and Class Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests as a result of its intrusions upon Plaintiff's and Class Members' privacy.

159. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiff and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

160. Plaintiff also seek such other relief as the Court may deem just and proper.

THIRD CAUSE OF ACTION
California Common Law Invasion of Privacy – Intrusion Upon Seclusion

161. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

162. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with Defendant via the Website and the communications platforms and services therein.

163. Plaintiff and Class Members communicated sensitive and protected medical information and personally identifiable information that they intended for only Defendant to receive and that they believed Defendant would keep private.

164. Defendant's disclosure of the substance and nature of those communications to third parties without the knowledge and consent of Plaintiff and Class Members is an intentional intrusion on Plaintiff's and Class Members' solitude or seclusion.

165. Plaintiff and Class Members had a reasonable expectation of privacy based on the sensitive nature of their communications. Plaintiff and Class Members have a general

expectation that their communications regarding health and finances will be kept confidential and not shared with a social media giant such as Facebook.

166. Defendant's disclosure of Plaintiff and Class Member's Private Information coupled with individually identifying information is highly offensive to the reasonable person.

167. As a result of Defendant's actions, Plaintiff and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

168. Plaintiff and Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

169. Plaintiff and Class Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests as a result of its intrusions upon Plaintiff's and Class Members' privacy.

170. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiff and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

171. Plaintiff also seeks such other relief as the Court may deem just and proper.

FOURTH CAUSE OF ACTION
Violation of the Unfair Competition Law – Unfair & Unlawful
(Cal. Bus. & Prof. Code § 17200, *et seq.*)

172. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

173. California's Unfair Competition Law ("UCL") prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

174. Defendant engaged in unlawful business practices in violation of the UCL in connection with its disclosure of Plaintiff's and Class Members' Private Information to unrelated third parties.

175. As alleged herein, Defendant's acts, omissions, and conduct constitute "business practices" within the meaning of the UCL.

176. Defendant violated the "unlawful" prong of the UCL by violating Plaintiff's and Class Members' constitutional rights to privacy and California Penal Code § 631(a).

177. Defendant's acts, omissions, and conduct also violates the unfair prong of the UCL because those acts, omissions, and conduct, as alleged herein, offended public policy (including the aforementioned state privacy statutes and laws) and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiff and Class Members.

178. The harm caused by the Defendant's conduct outweighs any potential benefits attributable to such conduct, and there were reasonably available alternatives to further Defendant's legitimate business interests. There is no business justification for aiding and enabling the interception of confidential information without adequately informing users in advance that the content of their communications will be shared with Facebook.

179. As a result of Defendant's violations of the UCL, Plaintiff and Class Members are entitled to injunctive relief. On information and belief, this is particularly true since the dissemination of Plaintiff's and Class Members' information is ongoing.

180. As a result of Defendant's violations of the UCL, Plaintiff and Class Members have suffered injury in fact and lost money or property. The unauthorized access to Plaintiff's and Class Members' private and personal data has diminished the value of that information. Plaintiff and the Class also derive economic value from their PII and would not have provided it to Defendant or Facebook for marketing purposes in the absence of consideration for that use. Thus, Defendant prevented Plaintiff and the Class from capturing the full value of their Personal Information for themselves.

181. In the alternative to those claims seeking remedies at law, Plaintiff and Class Members allege that there is no plain, adequate, and complete remedy that exists at law to address Defendant's unlawful and unfair business practices. The legal remedies available to Plaintiff are inadequate because they are not "equally prompt and certain and in other ways efficient" as equitable relief. *American Life Ins. Co. v. Stewart*, 300 U.S. 203, 214

(1937); *see also United States v. Bluitt*, 815 F. Supp. 1314, 1317 (N.D. Cal. Oct. 6, 1992) ("The mere existence' of a possible legal remedy is not sufficient to warrant denial of equitable relief."); *Quist v. Empire Water Co*., 2014 Cal. 646, 643 (1928) ("The mere fact that there may be a remedy at law does not oust the jurisdiction of a court of equity. To have this effect, the remedy must also be speedy, adequate, and efficacious to the end in view … It must reach the whole mischief and secure the whole right of the party in a perfect manner at the present time and not in the future."). Additionally, unlike damages, the Court's discretion in fashioning equitable relief is very broad and can be awarded in situations where the entitlement to damages may prove difficult. *Cortez v. Purolator Air Filtration Products Co.*, 23 Cal.4th 163, 177-180 (2000) (Restitution under the UCL can be awarded "even absent individualized proof that the claimant lacked knowledge of the overcharge when the transaction occurred."). Thus, restitution would allow recovery even when normal consideration associated with damages would not. *See, e.g., Fladeboe v. Am. Isuzu Motors Inc.*, 150 Cal. App. 4th 42, 68 (2007) (noting that restitution is available even in situations where damages may not be available). Furthermore, the standard for a violation of the UCL "unfair" prong is different from the standard that governs legal claims.

182. Therefore, Plaintiff and members of the proposed Class are entitled to equitable relief to restore them to a position they would have been in had Defendant not engaged in unfair competition, including an order enjoining Defendant's wrongful conduct,

restitution, and restitutionary disgorgement of all profits paid to Defendant as a result of its unlawful and unfair practices.

FIFTH CAUSE OF ACTION
Violation of the Electronic Communications Privacy Act
(18 U.S.C. § 2511(1)) ("ECPA")

183. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

184. The ECPA protects both the sending and receipt of communications.

185. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral, or electronic communication is intercepted.

186. A violation of the ECPA occurs where any person "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any . . . electronic communication" or "intentionally discloses, or endeavors to disclose, to any other person the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the [unlawful] interception of a[n] . . . electronic communication" or "intentionally uses, or endeavors to use, the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the [unlawful] interception of a[n] . . . electronic communication." 18 U.S.C. §§ 2511(1)(a), (c)-(d).

187. "Intercept" means "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

188. "Electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12).

189. "Contents" includes "any information relating to the substance, purport, or meaning" of the communication at issue. 18 U.S.C. § 2510(8).

190. By utilizing and embedding the Pixel on its Website, Defendant intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiff and Class Members, in violation of 18 U.S.C. § 2511(1)(a). Whenever Plaintiff and Class Members interacted with Defendant's Website, Defendant, through the Pixel source code it embedded and ran on its Website, contemporaneously and intentionally intercepted, and endeavored to intercept Plaintiff's and Class Members' electronic communications without authorization or consent.

191. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiff and Class Members to Facebook, while knowing or having reason to know that the information was obtained through the interception of an electronic

communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

192. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiff and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

193. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixel to intercept and disseminate Plaintiff's and Class Members' Private Information for financial gain.

194. Defendant was not acting under color of law to intercept Plaintiff's and the Class Members' wire or electronic communication.

195. Plaintiff and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiff's privacy via the Pixel tracking code.

196. Any purported consent that Defendant received from Plaintiff and Class Members was not valid.

197. Unauthorized Purpose – Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State – namely, invasion of privacy. The ECPA provides that a "party to the communication" may

liable where a "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C § 2511(2)(d).

198. Defendant is not a party to the communication based on its unauthorized duplication and transmission of communications with Plaintiff and the Class. *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 608 (9th Cir. 2020) (an entity's simultaneous, unknown duplication and forwarding of GET requests made to a web page's server does not qualify for the party exemption, because holding otherwise "would render permissible the most common methods of intrusion, allowing the exception to swallow the rule"). However, even assuming Defendant is a party, Defendant's simultaneous, unknown duplication, forwarding, and interception of Plaintiff's and Class Members' Private Information does not qualify for the party exemption.

199. Defendant is not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) on the ground that it was a participant in Plaintiff's and the Class Members' communications about their Private Information on its Website, because it used its participation in these communications to improperly share Plaintiff's and the Class Members' information with Facebook, a third-party that did not participate in these communications, that Plaintiff and the Class Members did not know was receiving their Private Information, and that Plaintiff and the Class Members did not consent to receive this information.

200. As a result of Defendant's violation of the ECPA, Plaintiff is entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

<u>SIXTH CAUSE OF ACTION</u>
Unjust Enrichment/Quasi-Contract

201. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

202. California law permits a standalone claim for unjust enrichment, allowing the court to construe the cause of action as a quasi-contract claim. *E.g., Astiana v. Hain Celestial Group, Inc.*, 783 F.3d 753, 756 (9th Cir. 2015).

203. California law recognizes a right to disgorgement of profits resulting from unjust enrichment, even where an individual has not suffered a corresponding loss. *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 599 (9th Cir. 2020).

204. California law requires disgorgement of unjustly earned profits regardless of whether a defendant's actions caused a plaintiff to directly expend his or her own financial resources or whether a defendant's actions directly caused the plaintiff's property to become less valuable.

205. Under California law, a stake in unjustly earned profits exists regardless of whether an individual planned to sell his or her data or whether the individual's data is made less valuable.

206. Plaintiff and Class Members retain a stake in the profits garnered from their Private Information because the circumstances are such that, as between Plaintiff and Class Members, on the one hand, and Defendant, on the other hand, it is unjust for Defendant to retain these profits.

207. By intercepting (and facilitating the interception), disclosing, and using for targeted advertising Plaintiff's and Class Members' Private Information and bundled with their other personal information, without their permission, Defendant generated revenues and was unjustly enriched at the expense of Plaintiff and the Class. It would be inequitable and unconscionable for Defendant to retain the profit, benefit, and other compensation it obtained via its impermissible wiretapping and data sharing practices.

208. Plaintiff and the Class Members seek an order from this Court requiring Defendant to disgorge all proceeds, profits, benefits, and other compensation obtained by Defendant from its improper and unlawful interception (and facilitating interception), disclosure, and use of their Private Information for targeted advertising.

209. Plaintiff and Class Members seek this equitable remedy because their legal remedies are inadequate. An unjust enrichment theory provides the equitable disgorgement

of profits even where an individual has not suffered a corresponding loss in the form of money damages.

RELIEF REQUESTED

210. Plaintiff, on behalf of herself and the proposed Class, respectfully requests that the Court grant the following relief:

a. Determine that the claims alleged herein may be maintained as a class action and issue an order certifying the Class defined above;

b. Appoint Plaintiff as the representative of the Class and counsel as Class counsel;

c. An order enjoining Defendant from engaging in the unlawful practices and illegal acts described herein;

d. An order awarding Plaintiff and the Class: (1) actual or statutory damages; (2) punitive damages—as warranted—in an amount to be determined at trial; (3) prejudgment interest on all amounts awarded; (4) equitable disgorgement and injunctive relief as pleaded or as the Court may deem proper; and (5) reasonable attorneys' fees and expenses and costs of suit pursuant to Cal. Code of Civil Procedure § 1021.5 and/or other applicable law; and

e. Other such and further relief as the Court may deem appropriate.

DEMAND FOR JURY TRIAL

211. Plaintiff, on behalf of herself and the proposed Class, demands a trial by jury for all triable claims asserted herein.

Dated: January 8, 2024 Respectfully submitted,

/s/ *John J. Nelson*

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
JOHN J. NELSON (SBN 317598)
jnelson@milberg.com
280 South Beverly Drive, Penthouse
Beverly Hills, California 90212
Tel: 872.365.7060