

1 **MILBERG COLEMAN BRYSON PHILLIPS**
2 **GROSSMAN, PLLC**
3 JOHN J. NELSON (SBN 317598)
4 jnelson@milberg.com
5 280 South Beverly Drive, Penthouse
6 Beverly Hills, California 90212
7 Tel: 872.365.7060

8 *Attorney for Plaintiff and the Class*

9 **UNITED STATES DISTRICT COURT**
10 **CENTRAL DISTRICT OF CALIFORNIA**

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

13 Plaintiff,

14 v.

15 POLICYGENIUS, LLC.,

16 Defendant.

17 Case No.

18 **CLASS ACTION COMPLAINT FOR:**

- 19 1. **CAL. PENAL CODE § 630, *et seq.***
- 20 2. **CAL. CONST. ART. 1 § 1**
- 21 3. **INTRUSION UPON SECLUSION**
- 22 4. **BUS. & PROF. CODE § 17200**
- 23 5. **18 U.S.C. § 2511(1) *et seq.***
- 24 6. **UNJUST ENRICHMENT**

1 Plaintiff Valerie Torres (“Plaintiff”) brings this class action complaint individually
2 and on behalf of all others similarly situated (“Class Members”) against Policygenius, LLC
3 (“Policygenius” or “Defendant”). The allegations contained in this class action complaint
4 are based on Plaintiff’s personal knowledge of facts pertaining to herself and upon
5 information and belief, including further investigation conducted by Plaintiff’s counsel.
6
7

8 NATURE OF THE ACTION

9 1. This is a class action lawsuit brought to address Defendant’s improper and
10 illegal disclosure of consumers’ personally identifiable information (“PII”) and/or
11 protected health information (“PHI”) (collectively referred to as “Private Information”) to
12 Meta Platforms, Inc. d/b/a Meta (“Facebook” or “Meta”) and other third parties as a result
13 of their use of Defendant’s website, www.policygenius.com (“Website”).
14
15

16 2. Information about a person’s physical, mental, and financial health is among
17 the most confidential and sensitive information in our society, and the mishandling of such
18 information can have serious consequences, including discrimination in the workplace or
19 denial of insurance coverage.
20

21 3. Defendant owns and controls www.policygenius.com, wherein customers are
22 asked to communicate highly personal and sensitive information in order to obtain quotes
23 for various types of life insurance and disability insurance.
24

25 4. At the outset, Policygenius assures Website users that their information will
26 be kept confidential, and the phrase “Your information is kept secure” appears next to an
27

1 image of a padlock on the Website’s homepage. The same phrase appears when users
2 navigate to the Policygenius life insurance questionnaire within the Website. Likewise, if
3 a user applies for disability insurance, the first page of that web survey states “We don’t
4 sell your personal information to third parties.”
5

6 5. Despite these representations, Defendant intentionally installed a tracking
7 pixel (the “Facebook Tracking Pixel” or “Pixel”) on its Website to surreptitiously duplicate
8 and send its customers’ private communications to Facebook, the contents of which include
9 Private Information and protected PHI/individually identifiable medical information.
10

11 6. By installing, programming, and controlling the Pixel as described herein,
12 Defendant aided, agreed, employed, and conspired with Facebook to intercept Plaintiff’s
13 and Class Members’ sensitive and private communications without their knowledge or
14 consent.
15

16 7. A pixel is a piece of code that “tracks the people and [the] type of actions they
17 take”¹ as they interact with a website, including how long a person spends on a particular
18 web page, which buttons the person clicks, which pages they view, and the text or phrases
19 they type into various portions of the website (such as a general search bar, chat feature, or
20 text box), among other things.
21
22
23
24
25
26

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

1 8. The Pixel is programmable, meaning that the Defendant is responsible for
2 determining which communications with the Website are tracked and transmitted to
3 Facebook.
4

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

10 10. Correspondingly, Defendant exploits the Private Information Plaintiff and
11 Class Members communicated to Defendant while seeking insurance coverage and uses
12 this Private Information to create detailed profiles that reflect individual consumer
13 preferences, allowing Facebook and Defendant to deliver targeted advertisements.
14
15

16 11. Defendant’s website, and more specifically its source code, manipulated
17 Plaintiff’s and Class Members’ web browsers so that their communications to Defendant
18 were automatically, contemporaneously, jointly, and surreptitiously sent to Facebook—an
19 unintended third-party recipient.
20

21 12. This is the functional equivalent of placing a bug or listening device on a
22 phone line because Defendant’s website allows third-parties to “listen in” and receive
23 communications in real time that Plaintiff intended only for Defendant.
24

25 13. Importantly, Facebook would not receive these communications but for
26 Defendant’s installation and implementation of the Pixel.
27
28

1 14. In addition to the Facebook Pixel, Defendant also installed and implemented
2 Facebook’s other Business Tools, such as the Conversions Application Programming
3 Interface (“Conversions API” or “CAPI”), on its Website.²
4

5 15. Unlike the Facebook Pixel, which co-opts a website user’s browser and forces
6 it to transmit information to Facebook in addition to the website owner, Conversions API
7 does not cause the user’s browser to transmit information directly to Facebook. Instead,
8 Conversions API tracks the user’s website interactions, including Private Information,
9 records and stores that information on the website owner’s servers, and then transmits the
10 data to Facebook from the website owner’s servers.^{3,4} Indeed, Facebook markets
11 Conversions API as a “better measure [of] ad performance and attribution across your
12 customer’s full journey, from discovery to conversion. This helps you better understand
13 how digital advertising impacts both online and offline results.”⁵
14
15
16
17
18

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

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

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

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

1 from this District. Plaintiff resides in this District, used defendant's Website in this District,
2 and her confidential communications were intercepted in this District.
3

4
5 **THE PARTIES**

6 **Plaintiff Valerie Torres**

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

9 23. In or about June 2022, Plaintiff Torres accessed www.policygenius.com
10 from her mobile device and used the website to search for life insurance quotes. In doing
11 so, Plaintiff provided Policygenius with her PII and health information. Plaintiff reasonably
12 expected that her communications with Policygenius via its website were confidential,
13 solely between herself and Policygenius, and that such communications would not be
14 transmitted to or intercepted by a third party.
15
16

17 24. Plaintiff Torres has an active Facebook account she regularly accesses
18 using her mobile device. As described herein, Policygenius sent Plaintiff's sensitive and
19 private PII and health information to third parties, including Facebook, when she accessed
20 Policygenius's website. Additionally, the information Policygenius sent to third parties was
21 linked to Plaintiff's Facebook ID.
22
23

24 25. Pursuant to the systematic process described herein, Policygenius assisted
25 third parties, including Facebook, with intercepting Plaintiff's communications, including
26 those that contained PII, protected health information, and related confidential information.
27
28

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

3
4 26. By failing to receive the requisite consent, Policygenius breached
5 confidentiality and unlawfully disclosed Plaintiff's personal, private, and personally
6 identifiable information and protected health information.

7
8
9 **Defendant**

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

16
17
18 **COMMON FACTUAL ALLEGATIONS**

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

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

25
26 29. Defendant uses the Website to connect Plaintiff and Class Members to
27

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

2 30. In order to understand Defendant’s unlawful data-sharing practices, it is
3 important first to understand basic web design and tracking tools.
4

5 ***Facebook’s Business Tools and the Pixel***

6
7 31. Facebook operates the world’s largest social media company and generated
8 \$117 billion in revenue in 2021, roughly 97% of which was derived from selling
9 advertising space.⁶
10

11 32. In conjunction with its advertising business, Facebook encourages and
12 promotes entities and website owners, such as Defendant, to utilize its “Business Tools”
13 to gather, identify, target, and market products and services to individuals.
14

15 33. Facebook’s Business Tools, including the Pixel and Conversions API, are bits
16 of code that advertisers can integrate into their webpages, mobile applications, and servers,
17 thereby enabling the interception and collection of user activity on those platforms.
18

19 34. The Business Tools are automatically configured to capture “Standard
20 Events” such as when a user visits a particular webpage, that webpage’s Universal
21 Resource Locator (“URL”) and metadata, button clicks, etc.⁷ Advertisers, such as
22

23
24 ⁶ FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS,
25 <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)

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

1 Defendant, can track other user actions and can create their own tracking parameters by
2 building a “custom event.”⁸

3
4 35. One such Business Tool is the Pixel which “tracks the people and type of
5 actions they take.”⁹ When a user accesses a webpage that is hosting the Pixel, their
6 communications with the host webpage are instantaneously and surreptitiously duplicated
7 and sent to Facebook’s servers—traveling from the user’s browser to Facebook’s server.

8
9 36. Notably, this transmission only occurs on webpages that contain the Pixel.
10 Thus, Plaintiff’s and Class Members’ Private Information would not have been disclosed
11 to Facebook via the Pixel but for Defendant’s decisions to install the Pixel on its Website.

12
13 37. Similarly, Plaintiff’s and Class Members’ Private Information would not have
14 been disclosed to Facebook via Conversions API but for Defendant’s decision to install
15 and implement that tool.

16
17 38. By installing and implementing both tools, Defendant caused Plaintiff’s and
18 Class Members’ communications to be intercepted and transmitted to Facebook via the
19

20
21 TRACKING, ADVANCED, <https://developers.facebook.com/docs/facebook-pixel/advanced/>;
22 *see also* FACEBOOK, BEST PRACTICES FOR FACEBOOK PIXEL SETUP,
<https://www.facebook.com/business/help/218844828315224?id=1205376682832142>;
23 FACEBOOK, APP EVENTS API, [https://developers.facebook.com/docs/marketing-api/app-](https://developers.facebook.com/docs/marketing-api/app-event-api/)
[event-api/](https://developers.facebook.com/docs/marketing-api/app-event-api/) (last visited Nov. 14, 2022).

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

27 ⁹ FACEBOOK, RETARGETING, <https://www.facebook.com/business/goals/retargeting>.

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

2 39. As explained below, these unlawful transmissions are initiated by Defendant's
3 source code concurrent with communications made via certain webpages.
4

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

8 40. Web browsers are software applications that allow consumers to navigate the
9 web and view and exchange electronic information and communications over the internet.
10 Each "client device" (such as computer, tablet, or smart phone) accesses web content
11 through a web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser,
12 Apple's Safari browser, and Microsoft's Edge browser).
13

14 41. Every website is hosted by a computer "server" that holds the website's
15 contents and through which the entity in charge of the website exchanges communications
16 with Internet users' devices via their web browsers.
17

18 42. Web communications consist of HTTP or HTTPS Requests and HTTP or
19 HTTPS Responses, and any given browsing session may consist of thousands of individual
20 HTTP Requests and HTTP Responses, along with corresponding cookies:
21

- 22 • **HTTP Request:** an electronic communication sent from the user device's browser
23 to the website's server. GET Requests are one of the most common types of HTTP
24 Requests. In addition to specifying a particular URL (i.e., web address), GET
25 Requests can also send data to the host server embedded inside the URL, and can
26
27

1 include cookies. POST Requests can send a large amount of data outside of the URL.
2 (For instance, uploading a PDF for filing a motion to a court)

- 3
- 4 • **Cookies:** a small text file that can be used to store information on the user device
5 which can later be communicated to a server or servers. Cookies are sent with HTTP
6 Requests from user devices to the host server. Some cookies are “third-party
7 cookies,” which means they can store and communicate data when visiting one
8 website to an entirely different website.
 - 9 • **HTTP Response:** an electronic communication that is sent as a reply to the user
10 device’s web browser from the host server in response to an HTTP Request. HTTP
11 Responses may consist of a web page, another kind of file, text information, or error
12 codes, among other data.¹⁰

13
14
15
16 43. A user’s HTTP Request essentially asks the Defendant’s Website to retrieve
17 certain information (such as the “Home-owners insurance” page). The HTTP Response
18 sends the requested information in the form of “Markup.” This is the foundation for the
19 pages, images, words, buttons, and other features that appear on the user’s screen as they
20 navigate Defendant’s Website.
21

22
23 44. Every website is comprised of Markup and “Source Code.” Source Code is
24 simply a set of instructions that commands the website visitor’s browser to take certain
25

26
27 ¹⁰ One browsing session may consist of hundreds or thousands of individual HTTP
28 Requests and HTTP Responses.

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

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

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

17 47. With substantial work and technical know-how, internet users can sometimes
18 circumvent this browser-based wiretap technology. This is why third parties bent on
19 gathering Personal Information, like Facebook, implement workarounds that savvy users
20 cannot evade. Facebook's workaround, for example, is called Conversions API.
21

1 Conversions API is an effective workaround because it does the transmission from their
2 own servers and does not rely on the User’s web browsers. Conversions API “is designed
3 to create a direct connection between [Web hosts’] marketing data and [Facebook].” Thus,
4 the communications between users and Defendant, which are necessary to use Defendant’s
5 Website, are actually received by Defendant and stored on its server before Conversions
6 API collects and sends the Private Information contained in those communications directly
7 from Defendant to Facebook. User devices do not have access to host servers and thus
8 cannot prevent (or even detect) this transmission.
9
10
11

12 48. While there is no way to confirm with certainty that a Web host like Defendant
13 has implemented workarounds like Conversions API without access to the host server,
14 companies like Facebook instruct Defendant to “[u]se the Conversions API in addition to
15 the [] Pixel, and share the same events using both tools,” because such a “redundant event
16 setup” allows Defendant “to share website events [with Facebook] that the pixel may
17 lose.”¹¹ Thus, it is reasonable to infer that Facebook’s customers who implement the
18 Facebook Pixel in accordance with Facebook’s documentation will also implement the
19 Conversions API workaround.
20
21

22 49. The third parties to whom a website transmits data through pixels and
23 associated workarounds do not provide any substantive content relating to the user’s
24
25

26 ¹¹ See
27 <https://www.facebook.com/business/help/308855623839366?id=818859032317965> (last
28 visited Jan. 23, 2023).

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

3
4 50. Thus, without any knowledge, authorization, or action by a user, a website
5 owner like Defendant can use its source code to commandeer the user’s computing device,
6 causing the device to contemporaneously and invisibly re-direct the users’ communications
7 to third parties.
8

9 51. In this case, Defendant employed the Tracking Pixel and Conversions API to
10 intercept, duplicate, and re-direct Plaintiff’s and Class Members’ Private Information to
11 Facebook.
12

13 52. For example, when a user visits www.policygenius.com and selects the
14 “Home” button under the “Compare quotes” banner, the user’s browser automatically
15 sends an HTTP Request to Defendant’s web server. Defendant’s web server automatically
16 returns an HTTP Response, which loads the Markup for that particular webpage. As
17 depicted below, the user only sees the Markup, not Defendant’s Source Code or underlying
18 HTTP Requests and Responses.
19
20
21
22
23
24
25
26
27
28

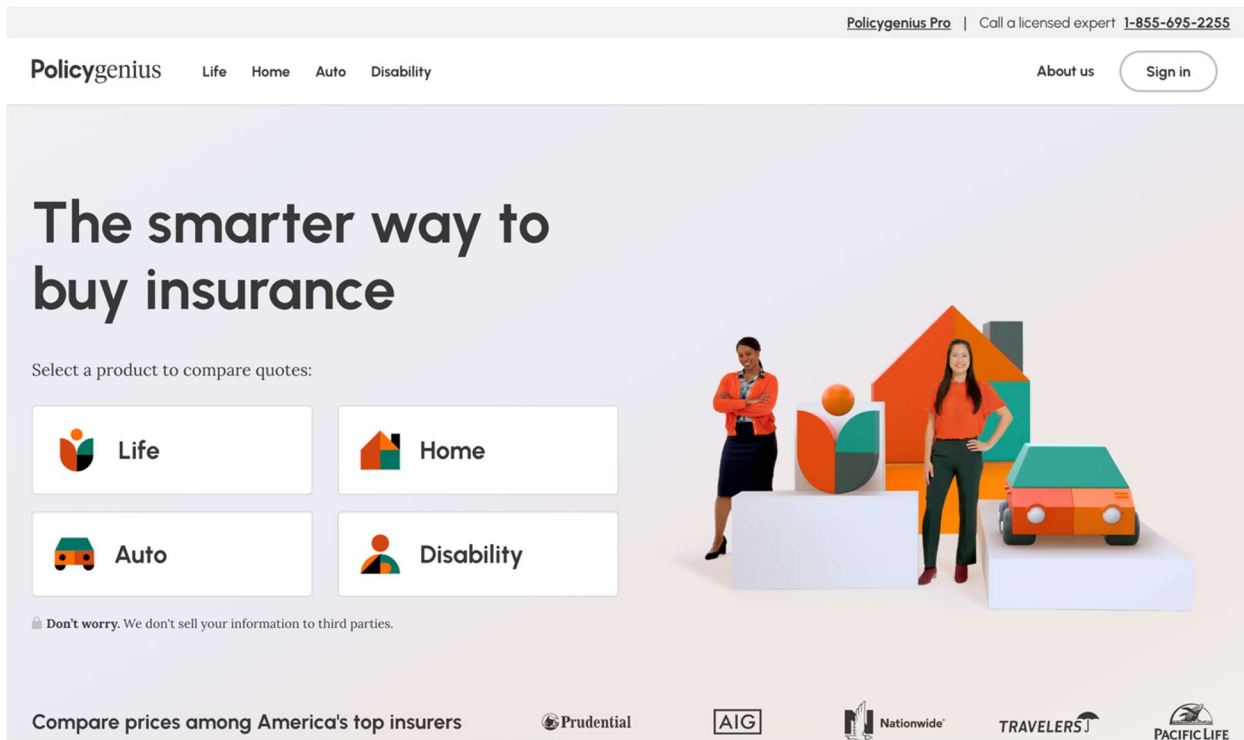


Figure 1. The image above is a screenshot taken from the user's web browser upon visiting www.policygenius.com (last accessed November 20, 2023).

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.

1 54. Defendant’s Source Code manipulates the user’s browser by secretly
2 instructing it to duplicate the user’s communications (HTTP Requests) with Defendant and
3
4 to send those communications to Facebook. These transmissions occur
5 contemporaneously, invisibly, and without the user’s knowledge.

6 55. Thus, without its users’ consent, Defendant has effectively used its source
7
8 code to commandeer and “bug” or “tap” its users’ computing devices, allowing Facebook
9 and other third parties to listen in on all of their communications with Defendant and
10 thereby intercept those communications, including Private Information.
11

12 56. Consequently, when Plaintiff and Class Members visit Defendant’s website
13 and communicate their Private Information, including, but not limited to, button clicks and
14 page visits are transmitted to third parties.
15

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

18 57. Defendant utilizes Facebook’s Business Tools and intentionally installed the
19 Pixel and Conversions API (“First Party cookies”) on its Website and servers to secretly
20 track users by recording their activity and experiences in violation of its common law,
21 contractual, statutory, and regulatory duties and obligations.¹³
22
23
24
25
26

27 ¹³ *Id.*

1 58. Defendant's Pixel has its own unique identifier (represented as
2 id=682897698520376), which can be used to identify which of Defendant's webpages
3 contain the Pixel.
4

5 59. The Pixel allows Defendant to optimize the delivery of ads, measure cross-
6 device conversions, create custom audiences, and decrease advertising and marketing
7 costs.¹⁴ However, Defendant's Website does not rely on the Pixel in order to function.
8

9 60. While seeking and using Defendant's services as an insurance provider,
10 Plaintiff and Class Members communicated their Private Information to Defendant via its
11 Website.
12

13 61. Plaintiff and Class Members were not aware that their Private Information
14 would be shared with Facebook as it was communicated to Defendant because, amongst
15 other things, Defendant did not disclose this fact.
16

17 62. Plaintiff and Class Members never consented, agreed, authorized, or
18 otherwise permitted Defendant to disclose their Private Information to Facebook, nor did
19 they intend for Facebook to be a party to their communications (many of them highly
20 sensitive and confidential) with Defendant.
21

22 63. Defendant's Pixel and First Party cookies sent non-public Private Information
23 to Facebook, including but not limited to Plaintiff's and Class Members': (1) desired
24 insurance coverage; (2) zip code; (3) residential address and status; and (4) policy status.
25
26

27 ¹⁴ *Id.*

1 64. Importantly, the Private Information Defendant’s Pixel sent to Facebook was
2 sent alongside the Plaintiff’s and Class Members’ Facebook ID (c_user cookie or “FID”),
3 thereby allowing individual users’ communications with Defendant, and the Private
4 Information contained in those communications, to be linked to their unique Facebook
5 accounts and therefore their identity.¹⁵
6

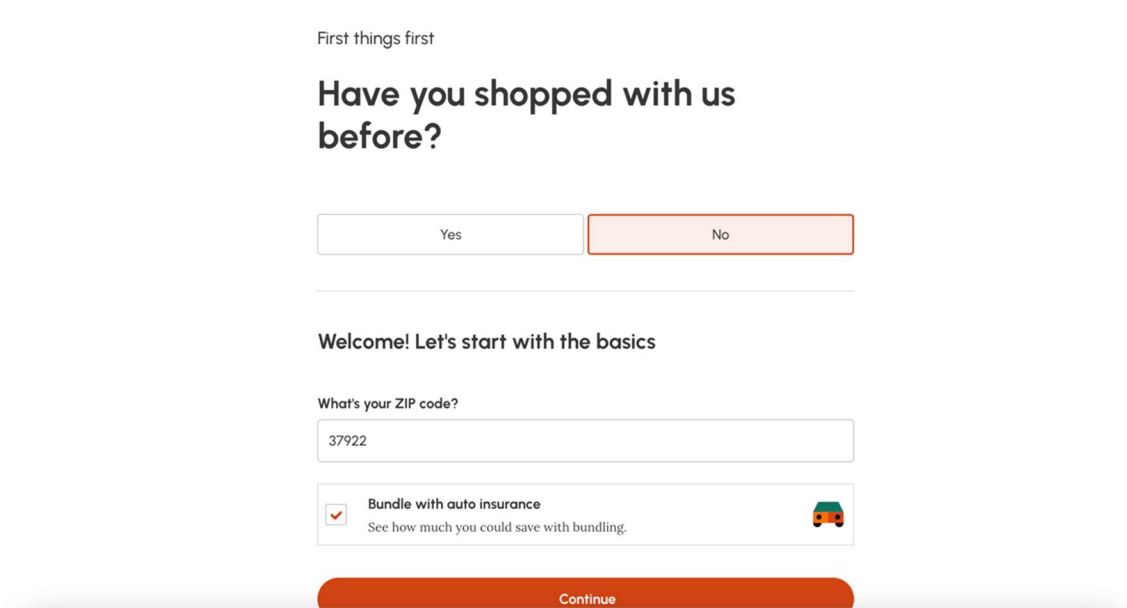
7
8 65. A user’s FID is linked to their Facebook profile, which generally contains a
9 wide range of demographic and other information about the user, including location,
10 pictures, personal interests, work history, relationship status, and other details. Because the
11 user’s Facebook ID uniquely identifies an individual’s Facebook account, Facebook—or
12 any ordinary person—can easily use the Facebook ID to locate, access, and view the user’s
13 corresponding Facebook profile quickly and easily.
14

15
16 66. Defendant deprived Plaintiff and Class Members of their privacy rights when
17 it: (1) implemented technology (i.e., the Facebook Pixel and First Party cookies) that
18 surreptitiously tracked, recorded, and disclosed Plaintiff’s and other online users’
19 confidential communications and Private Information; (2) disclosed users’ protected
20 information to Facebook—an unauthorized third-party; and (3) undertook this pattern of
21 conduct without notifying Plaintiff or Class Members and without obtaining their express
22 written consent.
23
24

25
26 ¹⁵ Defendant’s Website track and transmit data via first-party and third-party
27 cookies. The c_user cookie or FID is a type of third-party cookie assigned to each person
28 who has a Facebook account, and it is comprised by a unique and persistent set of numbers.

1 ***Defendant's Pixel Disseminates User Information via Its Website***

2
3 67. An example illustrates the point. If a user uses the Website to find home
4 insurance, Defendant's Website directs them to communicate Private Information,
5 including their zip code, and whether they own, rent, or are closing in the property they are
6 insuring. Unbeknownst to the patient, each and every communication is sent to Facebook
7 via Defendant's Pixel.
8

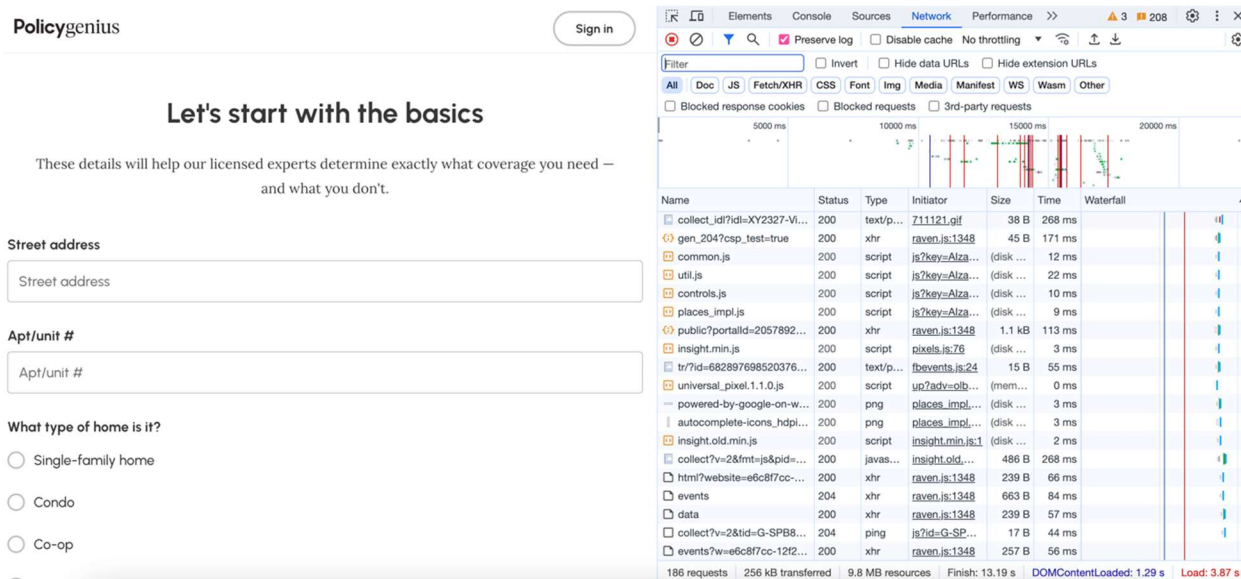


19
20 68. In the example above, the user is required to insert their home zip code before
21 being allowed to move onto the next page.

22 69. Next, the user is required to provide the status of the ownership of the property
23 they are seeking to insure, as well as their current home insurance agency and the length
24 of their policy. Additionally, users are required to submit the address of the property they
25
26
27
28

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

3
 4 70. Unbeknownst to ordinary users, this particular webpage—which is
 5 undoubtedly used to communicate Private Information for the purpose of seeking
 6 insurance—contains Defendant’s Pixel. The image below shows the “behind the scenes”
 7 portion of the website that is invisible to ordinary users. Importantly, each entry in the
 8 column represents just one instance in which Defendant’s Pixel sent this particular user’s
 9 information to Facebook.
 10 information to Facebook.
 11
 12



13
 14
 15
 16
 17
 18
 19
 20
 21
 22
 23 71. Thus, without alerting the user, Defendant’s Pixel sends each and every
 24 communication the user made via the webpage to Facebook, and the images below confirm
 25
 26
 27
 28

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

- 3
- 4 ▪ **url:**
 - 5 ▪ `https://www.facebook.com/tr?id=682897698520376&ev=Lead`
- 6 ▪ **query String:**
 - 7 ▪ `id: 682897698520376`
 - 8 ▪ `ev: Lead`
- 9 ▪ **cookies:**
 - 10 ▪ `sb: vG6FYo6agRKDbm8QWCARBy76`
 - 11 ▪ `datr: XleNYt2e1ma70z6Yn8mguXwb`
 - 12 ▪ `c_user: [REDACTED]`
 - 13 ▪ `usida: eyJ2ZXliOjEsImkljoiQXJvcjhwM2QybjiZyIsInRpbWUiOjE2NzQxNjg1MTI9`
 - 14 ▪ `xs: 44:U196GIVHcrlioA:2:1673030231:-1:12847::AcVOEc0LopXA4541AiiTFIB0GruPV6abkh9s2kyAaWw`
 - 15 ▪ `fr: 0nJKU0mxhi7gRIbbX.AWX6sbxcW5pYZyPw5MvmzYv2etY.Bjz0bf.zo.AAA.0.0.Bjz0bf.AWW5kb59KO0`
 - 16 ▪ `dpr: 2`

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

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

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

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

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

8 **76.** Facebook receives at least six cookies when Defendant’s website transmits
 9 information via the Pixel:
 10
 11
 12

AID	AJHaeXlqicIHZVBEdlZe-ntMoc46hqF3fC7GtZ...	.googl...	/ads	2024-...	61	✓	✓	None	Medium
TDCPM	CAESFgoHcnViaWNVbhlLCJ2jMPiXa08EAUSF...	.adsrv...	/	2024-...	1141		✓	None	Medium
TDID	eabb3d7b-17a5-42d9-9aeb-537eefdda44a	.adsrv...	/	2024-...	40		✓	None	Medium
presence	C%7B%22i3%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.Cj0KQCIApOyqBhDIARIsAGf...	.poli...	/	2024-...	114				Medium
AEC	Ackid1Tmt1ICxFPgyJdubtzpLMWkI1EGtswiko...	.googl...	/	2024-...	61	✓	✓	Lax	Medium
datr	_LPfZPwofp4WaZTExcnHozl	.faceb...	/	2024-...	28	✓	✓	None	Medium
pt	v2:6ec3e6b4fd8baf9a4b8d02cabcc42405b288...	.ispt...	/	2024-...	134		✓	None	Medium
_fbp	fb.1.1700510930674.1416019771	.poli...	/	2024-...	33			Lax	Medium
lms_analytics	AQEg2QEHT9cNwAAAYvuWagFefNf3oya_SD0...	.linke...	/	2023-...	109		✓	None	Medium
__cf_bm	hfYswD4nFTW46kfbssDklynzAPg18zx1Z7hyN6...	.hubs...	/	2023-...	152	✓	✓	None	Medium
Conversion	EgwIABUAAAAAHQAAAAAYASC_I43Qn5WAYxl...	www....	/page...	2024-...	400		✓	None	Medium
_uetsid	a07fc77087e011ead5bf5ed89d2bc83	.poli...	/	2023-...	39				Medium
SEARCH_SAMESITE	CgQlx5kB	.googl...	/	2024-...	23			Strict	Medium
_cfuvid	ho3d5ir6y9rEjMxRyQmaXIUWQ8fQA6FQ7FaPa...	.hubs...	/	Session	76	✓	✓	None	Medium
NID	511=MYulSaZT_WTO3r579sdNVPMiluSAF4pk...	.googl...	/	2024-...	279	✓	✓	None	Medium
UserMatchHistory	AQJ98GkrUdsURQAAAYvuWabmwh_OmjQIWT...	.linke...	/	2023-...	367		✓	None	Medium
li_sugr	b2f08509-12dd-4238-a91f-bf8bcfb06719	.linke...	/	2024-...	43		✓	None	Medium
trckshesh	c9d4ae95-38a3-4523-b1a7-890cb1b20549	www....	/	Session	44				Medium
AnalyticsSyncHistory	AQJJI79m1IA1QAAAYvuWabmuTg6l232fSZZq0...	.linke...	/	2023-...	106		✓	None	Medium
__pdst	45bd8fe09c794ec9b69cb1bd2f6f8b7	www....	/	2024-...	38			Strict	Medium
fpc	df332de2-9a8c-4c28-8c03-1e62f0ede7aa	www....	/	2023-...	39				Medium
ajs_anonymous_id	5a47cf39-2701-41a6-actf7-0dae0e4160a3	.poli...	/	2024-...	52			Lax	Medium

1 77. When a visitor’s browser has recently logged out of an account, Facebook
 2 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

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

12 79. The cookies listed in the two images above are commonly referred to as third-
 13 party cookies because they were “created by a website with a domain name other than the
 14 one the user is currently visiting”—i.e., Facebook. Although Facebook created these
 15 cookies, Defendant is ultimately responsible for the manner in which individual website
 16 users were identified via these cookies, and Facebook would not have received this data
 17 but for Defendant’s implementation and use of the Pixel throughout its website.
 18
 19
 20
 21
 22

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

26 ¹⁷ Data Protection Commissioner, Facebook Ireland Ltd: Report of Re-Audit (Sept.
 27 21, 2012), p. 33, http://www.europe-v-facebook.org/ODPC_Review.pdf (last visited May
 28 11, 2023).

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

1 80. Defendant also revealed its website visitors’ identities via first-party cookies
 2 such as the `_fbp` cookie that Facebook uses to identify a particular browser and a user:¹⁹
 3

<code>datr</code>	<code>_LPfZPwoFp4WaZTExcnhoZl</code>	<code>.faceb...</code>	<code>/</code>	2024-...	28	✓	✓	None	Medium
<code>pt</code>	<code>v2:6ec3e6b4fd8baf9a4b8d02cabcc42405b288...</code>	<code>.isport.tv</code>	<code>/</code>	2024-...	134		✓	None	Medium
<code>_fbp</code>	<code>fb.1.1700510930674.1416019771</code>	<code>.poli...</code>	<code>/</code>	2024-...	33			Lax	Medium
<code>lms_analytics</code>	<code>AQEg2QEHT9cNwAAAYvuWagFeNf3oya_SD0...</code>	<code>.linke...</code>	<code>/</code>	2023-...	109			None	Medium
<code>_cf_bm</code>	<code>hfySwD4nFTW46kfbssDklynzAPg18zx1Z7hyN6...</code>	<code>.hubs...</code>	<code>/</code>	2023-...	152	✓	✓	None	Medium
<code>Conversion</code>	<code>FnwIARIIAAAAAHQAAYASC: i43Qn5WAxvl</code>	<code>www</code>	<code>/page</code>	2024-	400		✓	None	Medium

6
7
8 81. Importantly, the `_fbp` cookie is transmitted to Facebook even when the user’s
 9 browser is configured to block third-party tracking cookies because, unlike the `fr` cookies
 10 and `c_user` cookie, the `_fbp` cookie functions as a first-party cookie—i.e. a cookie that was
 11 created and placed on the website by Defendant.²⁰
 12

13 82. The Facebook Tracking Pixel uses both first- and third-party cookies.
 14

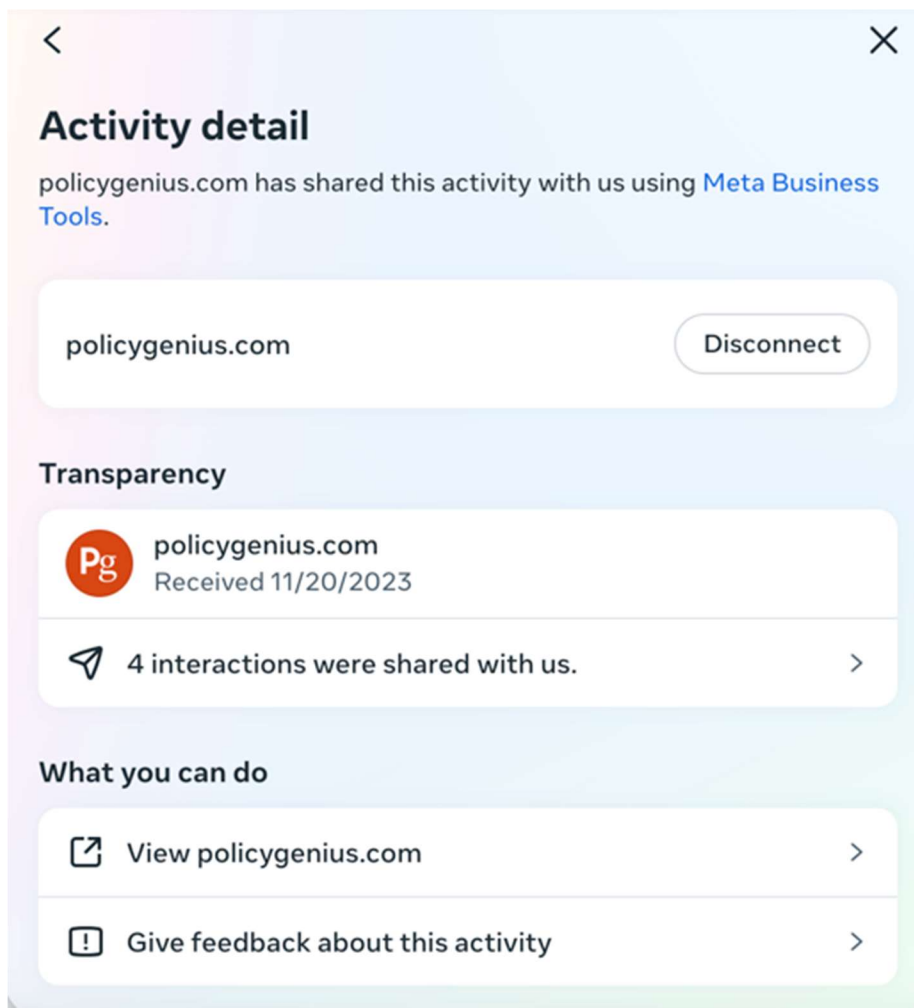
15 83. In summation, Facebook, at a minimum, uses the `fr`, `_fbp`, and `c_user` cookies
 16 to link website visitors’ communications and online activity with their corresponding
 17 Facebook profiles, and, because the Pixel is automatically programmed to transmit data via
 18 both first-party and third-party cookies, users’ information and identities are revealed to
 19 Facebook even when they have disabled third-party cookies within their web browsers.
 20

21 84. The image below, gathered from a website visitor’s own Facebook account
 22 after the fact, makes it patently clear that Defendant is actively sending patient
 23

24
25 ¹⁹ *Id.*

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

1 communications to Facebook, stating Policygenius shared the user’s information four
2 times using Facebook business tools.
3



4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20 85. At present, the full breadth of Defendant’s tracking and data sharing practices
21 is unclear, but other evidence suggests Defendant is using additional tracking pixels and
22 tools to transmit its users’ Private Information to additional third parties. For example, the
23 image below indicates that Defendant is also sending its users’ protected health information
24 to Google via Google Tag Manager.
25
26
27
28

1 86. The image below contains the URL the user visited was sent to Google, and
 2 Defendant does not appear to have enabled the anonymize feature provided by Google
 3 because the text “aip:” does not appear in the image.
 4

Request URL:	https://www.googletagmanager.com/gtm.js?id=GTM-5PWJJP&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

5
6
7
8
9
10
11
12
13
14 87. Accordingly, Google receives users’ communications alongside the users’ IP
15 address, which is also impermissible under HIPAA.
16

17 88. Defendant does not disclose that the Pixel, First Party cookies, Google Tag
18 Manager, or any other tracking tools embedded in the Website’s source code tracks,
19 records, and transmits Plaintiff’s and Class Members’ Private Information to Facebook and
20 Google. Moreover, Defendant never received consent or written authorization to disclose
21 Plaintiff’s and Class Members’ private communications to Facebook or Google
22

23 **A. Facebook Exploited and Used Plaintiff’s and Class Members’ Private**
 24 **Information**
 25
 26
 27
 28

1 89. Unsurprisingly, Facebook does not offer its Pixel to companies like Defendant
2 solely for Defendant’s benefit. “Data is the new oil of the digital economy,”²¹ and Facebook
3 has built its more-than \$300 billion market capitalization on mining and using that “digital”
4 oil. Thus, the large volumes of personal and sensitive health-related data Defendant
5 provides to Facebook are actively examined, curated, and put to use by the company.
6 Facebook acquires the raw data to transform it into a monetizable commodity, just as an
7 oil company acquires crude oil to transform it into gasoline. Indeed, Facebook offers the
8 Pixel free of charge²² and the price that Defendant pays for the pixel is the data that it
9 allows Facebook to collect.
10
11
12

13 90. Facebook describes itself as a “real identity platform,”²³ meaning users are
14 allowed only one account and must share “the name they go by in everyday life.”²⁴ To that
15 end, when creating an account, users must provide their first and last name, date of birth,
16 and gender.²⁵
17
18
19
20
21

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

24 ²² <https://seodigitalgroup.com/facebook-pixel/> (last visited November 27, 2023).

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

27 ²⁴ FACEBOOK, COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY,
28 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).

1 91. Facebook sells advertising space by emphasizing its ability to target users.²⁶
2 Facebook is especially effective at targeting users because it surveils user activity both on
3 and off its site (with the help of companies like Defendant).²⁷ This allows Facebook to
4 make inferences about users beyond what they explicitly disclose, including their
5 “interests,” “behavior,” and “connections.”²⁸ Facebook compiles this information into a
6 generalized dataset called “Core Audiences,” which advertisers use to apply highly specific
7 filters and parameters for their targeted advertisements.²⁹
8

9
10 92. Advertisers can also build “Custom Audiences,”³⁰ which helps them reach
11 “people who have already shown interest in [their] business, whether they’re loyal
12 customers or people who have used [their] app or visited [their] website.”³¹ With Custom
13
14
15

16 ²⁶ FACEBOOK, WHY ADVERTISE ON FACEBOOK,
17 <https://www.facebook.com/business/help/205029060038706> (last visited November 27,
18 2023).

19 ²⁷ FACEBOOK, ABOUT FACEBOOK PIXEL,
20 <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>
21 (last visited November 27, 2023).

22 ²⁸ FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR
23 BUSINESS, <https://www.facebook.com/business/ads/ad-targeting> (last visited November
24 27, 2023).

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

28 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).

1 Audiences, advertisers can target existing customers directly, and they can also build
2 “Lookalike Audiences,” which “leverages information such as demographics, interests,
3 and behavior from your source audience to find new people who share similar qualities.”³²
4

5 Unlike Core Audiences, Custom Audiences and Lookalike Audiences are only available if
6 the advertiser has sent its underlying data to Facebook. This data can be supplied to
7 Facebook by manually uploading contact information for customers or by utilizing
8 Facebook’s “Business Tools.”³³
9

10 93. The Facebook Pixel, and the personal data mined and curated with it, is key
11 to this business. As Facebook puts it, the Business Tools “help website owners and
12 publishers, app developers and business partners, including advertisers and others,
13 integrate with Facebook, understand and measure their products and services, and better
14 reach and serve people who might be interested in their products and services.”³⁴
15
16

17 94. Facebook does not merely collect information gathered by the Pixel and store
18 it for safekeeping on its servers without ever accessing the information. Instead, in
19 accordance with the purpose of the Pixel to allow Facebook to create Core, Custom, and
20
21

22 _____
23 ³² Facebook, About Lookalike Audiences,
24 <https://www.facebook.com/business/help/164749007013531?id=401668390442328> (last
25 visited November 27, 2023).

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

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

1 Lookalike Audiences for advertising and marketing purposes, Facebook viewed,
2 processed, and analyzed Plaintiff's and Class Members' confidential Private Information.
3
4 Upon information and belief, such viewing, processing, and analyzing was performed by
5 computers and/or algorithms programmed and designed by Facebook employees at the
6 direction and behest of Facebook.
7

8 95. Facebook receives over four petabytes of information every day and must rely
9 on analytical tools designed to view, categorize, and extrapolate the data to augment human
10 effort.³⁵ This process is known as data ingestion and allows “businesses to manage and
11 make sense of large amounts of data.”³⁶
12

13 96. By using these tools, Facebook is able to rapidly translate the information it
14 receives from the Pixel to display relevant ads to consumers. For example, if a consumer
15 visits a retailer's webpage and places an item in their shopping cart without purchasing it,
16 the next time the shopper visits Facebook, an ad for that item will appear on the shopper's
17 Facebook page.³⁷ This evidences that Facebook views and categorizes data as they are
18 received from the Pixel.
19
20

21 97. Moreover, even if Facebook eventually deletes or anonymizes sensitive
22 information that it receives, it must first view that information to identify it as containing
23

24
25 ³⁵ <https://medium.com/@srank2000/how-facebook-handles-the-4-petabyte-of-data-generated-per-day-ab86877956f4> (last visited November 27, 2023).

26 ³⁶ <https://scaleyourapp.com/what-database-does-facebook-use-a-1000-feet-deep-dive/>
27 (last visited November 27, 2023).

28 ³⁷ <https://www.oberlo.com/blog/facebook-pixel> (last visited November 27, 2023).

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

3
4 **B. Defendant Was Enriched and Benefitted from the Use of The Pixel and**
5 **Unauthorized Disclosures and Plaintiff's and Class Members' Data and**
6 **Private Information Had Financial Value**

7 98. The primary motivation and a determining factor in Defendant's interception
8 and disclosure of Plaintiff's and Class Members' Private Information was to commit
9 tortious acts as alleged herein; namely, the use of Private Information for advertising in the
10 absence of express written consent. Defendant's further use of the Private Information after
11 the initial interception and disclosure for marketing and revenue generation was an
12 invasion of privacy.
13

14
15 99. In exchange for disclosing the Private Information of its users, Defendant is
16 compensated by Facebook in the form of enhanced advertising services and more cost-
17 efficient marketing on its platform.
18

19 100. Retargeting is a form of online marketing that targets users with ads based on
20 their previous internet communications and interactions. Upon information and belief, as
21 part of its marketing campaign, Defendant re-targeted customers and potential customers.
22

23 101. Upon information and belief, Defendant was advertising its services on
24 Facebook, and the Pixel was used to help Defendant understand the success of its
25 advertisement efforts on Facebook. Defendant, in coordination with Facebook, associated
26
27
28

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

3
4 102. By utilizing the Pixel, the cost of advertising and retargeting was reduced,
5 thereby benefitting Defendant.

6 103. Defendant's disclosure of Private Information also hurt Plaintiff and the Class.
7
8 Conservative estimates suggest that in 2018, Internet companies earned \$202 per American
9 user from mining and selling data. That figure will keep increasing, and estimates are as
10 high as \$434 per user, for a total of more than \$200 billion industry wide.

11
12 104. The value of health data in particular is well-known and has been reported on
13 extensively in the media. For example, Time Magazine published an article in 2017 titled
14 "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry," in which it
15 described the extensive market for health data and observed that the market for information
16 was both lucrative and a significant risk to privacy.³⁸

17
18 105. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-
19 identified patient data has become its own small economy: There's a whole market of
20 brokers who compile the data from providers and other health-care organizations and sell
21 it to buyers."³⁹
22
23
24
25

26 ³⁸ See <https://time.com/4588104/medical-data-industry/> (last visited November 27, 2023).

27 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).

1 106. Indeed, numerous marketing services and consultants offering advice to
2 companies on how to build their email and mobile phone lists—including those seeking to
3 take advantage of targeted marketing—direct putative advertisers to offer consumers
4 something of value in exchange for their personal information. “No one is giving away
5 their email address for free. Be prepared to offer a book, guide, webinar, course or
6 something else valuable.”⁴⁰
7
8

9 107. There is also a market for data in which consumers can participate. Personal
10 information has been recognized by courts as extremely valuable. *See In re Marriott Int’l,*
11 *Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) (“Neither
12 should the Court ignore what common sense compels it to acknowledge—the value that
13 personal identifying information has in our increasingly digital economy. Many
14 companies, like Marriott, collect personal information. Consumers too recognize the value
15 of their personal information and offer it in exchange for goods and services.”).
16
17

18 108. Several companies have products through which they pay consumers for a
19 license to track their data. Google, Nielsen, UpVoice, HoneyGain, and SavvyConnect are
20 all companies that pay for browsing history information.
21

22 109. Meta itself has paid users for their digital information, including browsing
23 history. Until 2019, Meta ran a “Facebook Research” app through which it paid \$20 a
24

25
26 ⁴⁰ Vero, How to Collect Emails Addresses on Twitter (June 2014), available at
27 <https://www.getvero.com/resources/twitter-lead-generation-cards/> (last visited November
28 27, 2023).

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

3
4 110. Additionally, healthcare data may be valued at up to \$250 per record on the
5 black market.⁴¹

6
7 **TOLLING OF THE STATUTE OF LIMITATIONS & DELAYED DISCOVERY**

8 111. All applicable statute(s) of limitations have been tolled by the delayed
9 discovery doctrine. Plaintiff and Class Members could not have reasonably discovered
10 Facebook's practice of tracking and intercepting their activities and communications on
11 Defendant's website until this class action litigation commenced.
12

13 112. Plaintiff did not learn of Facebook's interception of their activities and
14 communications on Defendant's website until being informed by the undersigned counsel
15 of record before this complaint was filed.
16

17 113. Plaintiff had no reason to believe her Private Information was being
18 intercepted through Defendant's website at all, let alone in real time while Plaintiff was
19 inputting information into Defendant's website but before Plaintiff submitted her
20 application. As detailed above, Defendant's privacy policy hyperlinks were buried on the
21 bottom of Defendant's homepage, and Plaintiff was not presented with a conspicuous
22 clickwrap listing the privacy policy hyperlinks. Furthermore, the technologies Defendant
23
24

25
26 ⁴¹ Tori Taylor, *Hackers, Breaches, and the Value of Healthcare Data*, *SecureLink* (June
27 30, 2021), <https://www.securelink.com/blog/healthcare-data-new-prize-hackers> (last
28 visited November 27, 2023).

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

3
4 114. As a result, any and all applicable statutes of limitations otherwise applicable
5 to the allegations herein have been tolled.

6
7 **CLASS ACTION ALLEGATIONS**

8 115. **Class Definition:** Pursuant to Rule 23 of the Federal Rules of Civil Procedure,
9 Plaintiff brings this action on behalf of herself and other similarly situated individuals
10 defined as: all persons in California who, during the class period, provided their personally
11 identifiable information and/or health information to Policygenius using
12 www.policygenius.com (the “Class”).
13

14 116. Plaintiff reserves the right to modify the class definitions or add sub-classes
15 as necessary prior to filing a motion for class certification, at class certification, or at any
16 later time as the Court permits.
17

18 117. The “Class Period” is the time period beginning on the date established by the
19 Court’s determination of any applicable statute of limitations, after consideration of any
20 tolling, concealment, and accrual issues, and ending on the date of entry of judgement.
21

22 118. Excluded from the Class is Policygenius; any affiliate, parent, or subsidiary
23 of Policygenius; any entity in which Policygenius has a controlling interest; any officer
24 director, or employee of Policygenius; any successor or assign of Policygenius; anyone
25
26
27
28

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

3
4 119. Numerosity/Ascertainability. Members of the Class are so numerous that
5 joinder of all members would be unfeasible and not practicable. The exact number of Class
6 Members is unknown to Plaintiff at this time. However, it is estimated that there are
7 thousands of individuals in the Class. The identity of such membership is readily
8 ascertainable from Policygenius's records and non-parties' records.
9

10
11 120. Typicality. Plaintiff's claims are typical of the claims of the Class because
12 Plaintiff used www.policygenius.com and had their Private Information disclosed to third
13 parties without their express written authorization or knowledge. Plaintiff's claims are
14 based on the same legal theories as the claims of other Class Members.
15

16 121. Adequacy. Plaintiff is fully prepared to take all necessary steps to represent
17 fairly and adequately the interests of the Class Members. Plaintiff's interests are coincident
18 with, and not antagonistic to, those of the Class Members. Plaintiff is represented by
19 attorneys with experience in the prosecution of class action litigation generally and in the
20 emerging field of digital privacy litigation specifically. Plaintiff's attorneys are committed
21 to vigorously prosecuting this action on behalf of the Class Members.
22

23
24 122. Common Questions of Law and Fact Predominate/Well Defined Community
25 of Interest. Questions of law and fact common to the Class Members predominate over
26 questions that may affect only individual Class Members because Defendant has acted on
27

1 grounds generally applicable to the Class. Such generally applicable conduct is inherent in
2 Defendant's wrongful conduct. The following questions of law and fact are common to
3 the Class:
4

- 5 a. Whether Plaintiff and Class Members had a reasonable expectation of privacy
6 under the circumstances;
- 7
- 8 b. Whether Defendant's website surreptitiously records personally identifiable
9 information, protected health information, financial information, and related
10 communications and subsequently, or simultaneously, discloses that
11 information to third parties;
- 12
- 13 c. Whether Defendant disseminated Class Members' confidential
14 communications to third parties;
- 15
- 16 d. Whether Policygenius's conduct resulted in a breach of confidentiality;
- 17
- 18 e. Whether Policygenius violated Plaintiff's and Class Members' privacy rights
19 by using software to record and communicate website visitor's personally
20 identifiable information, including unique identifiers and FIDs, alongside
21 confidential medical communications;
- 22
- 23 f. Whether Plaintiff and Class Members are entitled to damages under CIPA,
24 ECPA, or any other relevant statute;
- 25
- 26 g. Whether Defendant's actions violate Plaintiff's and Class Members' privacy
27 rights as provided by the California Constitution; and
28

1 h. Whether Defendant's actions violated California's Unfair Competition Law,
2 Bus. and Prof. Code § 17200 *et seq.* by, among other things, surreptitiously
3 recording personally identifiable information, protected health information,
4 financial information, and related communications and subsequently, or
5 simultaneously, disclosing that information to third parties.
6

7
8 123. Superiority. Class action treatment is a superior method for the fair and
9 efficient adjudication of the controversy. Such treatment will permit a large number of
10 similarly situated persons to prosecute their common claims in a single forum
11 simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or
12 expense that numerous individual actions would engender. The benefits of proceeding
13 through the class mechanism, including providing injured persons a method for obtaining
14 redress on claims that could not practicably be pursued individually, substantially
15 outweighs potential difficulties in management of this class action. Plaintiff is unaware of
16 any special difficulty to be encountered in litigating this action that would preclude its
17 maintenance as a class action.
18
19
20

21
22 **CLAIMS FOR RELIEF**

23 **FIRST CAUSE OF ACTION**

24 **Violation Of the California Invasion of Privacy Act,**
25 **Cal. Penal Code § 630, *et seq***

26 124. Plaintiff repeats the allegations contained in the paragraphs above as if fully
27 set forth herein and brings this count individually and on behalf of the proposed Class.
28

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

3
4
5 The Legislature hereby declares that advances in science and technology have
6 led to the development of new devices and techniques for the purpose of
7 eavesdropping upon private communications and that the invasion of privacy
8 resulting from the continual and increasing use of such devices and techniques
9 has created a serious threat to the free exercise of personal liberties and cannot
10 be tolerated in a free and civilized society.

11 Cal. Penal Code § 630.

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

13 Any person who, by means of any machine, instrument, or contrivance, or in
14 any other manner ... [ii] willfully and without the consent of all parties to the
15 communication, or in any unauthorized manner, reads, or attempts to read, or
16 to learn the contents or meaning of any message, report, or communication
17 while the same is in transit or passing over any wire, line, or cable, or is being
18 sent from, or received at any place within this state; [iii] or who uses, or
19 attempts to use, in any manner, or for any purpose, or to communicate in any
20 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).

21 127. A defendant must show it had the consent of all parties to a communication.

22 128. Plaintiff’s and Class Members’ specific user input events and choices and
23 information typed on Defendant’s website are tracked by Defendant using the SDK
24 provided by third parties, such as Facebook. The user’s affirmative actions, such as
25
26
27
28

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

3
4 129. At all relevant times, Defendant aided, agreed with, and conspired with third
5 parties, such as Facebook, to track and intercept Plaintiff's and Class Members' internet
6 communications while accessing www.policygenius.com. These communications were
7 intercepted without the authorization and consent of Plaintiff and Class Members.
8

9 130. Defendant intentionally inserted an electronic device into its website that,
10 without the knowledge and consent of Plaintiff and Class Members, tracked and
11 transmitted the substance of their confidential communications with Defendant to a third
12 party.
13

14 131. Defendant willingly facilitated Facebook's interception and collection of
15 Plaintiff's and Class Members' Private Information by embedding the Facebook Pixel on
16 its website.
17

18 132. Defendant intended to share Plaintiff's and Class Members' private and
19 personal information and communications to help the third parties learn some meaning of
20 the content of the communications.
21

22 133. Plaintiff and Class Members are residents of California and used their devices
23 within California. As such, Defendant records and disseminates Plaintiff's and Class
24 Members' data, communications, and personal information in California.
25
26
27

1 134. Plaintiff and Class Members did not consent to any of Defendant’s actions in
2 implementing the tracking software. Nor have Plaintiff or Class Members consented to
3 Defendant’s intentional collection and sharing of Plaintiff’s and Class Members’ electronic
4 communications, personally identifiable information, medical information, or financial
5 information.
6

7
8 135. At all relevant times to this complaint, Plaintiff and the other Class Members
9 did not know Defendant was engaging in such recording and sharing of information, and
10 therefore could not provide consent to have any part of their private and confidential
11 communications, personally identifiable information, financial information, and/or
12 medical information intercepted and recorded by Defendant and thereafter transmitted to
13 others.
14

15
16 136. The following items constitute “machine[s], instrument[s], or contrivance[s]”
17 under the CIPA, and even if they do not, the software in the source code of Policygenius’s
18 website, such as the Facebook Tracking Pixel, falls under the broad catch-all category of
19 “any other manner”:
20

- 21 a. The computer codes and programs third parties, such as Facebook, used to
22 track Plaintiff’s and Class Members’ communications while they were
23 navigating www.policygenius.com;
24
25 b. Plaintiff’s and Class Members’ browsers;
26
27 c. Plaintiff’s and Class Members’ computing and mobile devices;
28

- 1 d. Facebook’s web and ad servers;
- 2 e. The web and ad-servers from which third parties, including Facebook, tracked
- 3 and intercepted Plaintiff’s and Class Members’ communications while they
- 4 were using a web browser to access or navigate www.policygenius.com; and
- 5
- 6 f. The computer codes and programs used by third parties, including Facebook,
- 7 to effectuate its tracking and interception of Plaintiff’s and Class Members’
- 8 communications while they were using a browser to visit Defendant’s
- 9 website.
- 10
- 11

12 137. Defendant fails to disclose that it is using software from third parties, such as
13 Facebook Pixel, specifically to track and automatically and simultaneously transmit
14 communications, personally identifiable information, and protected health information to
15 a third parties, *e.g.*, Facebook. Defendant is aware that these communications are
16 confidential as its “Privacy Policy” acknowledges the confidential nature of private
17 medical information but fails to disclose to website visitors who submit an insurance quote
18 that Policygenius will record and provide their private and personal information with third
19 parties.
20
21

22 138. The private information that Defendant transmits while using third party
23 software, such as Facebook Pixel, including medical information consumers enter into the
24 website, IP addresses, phone numbers and home addresses constitute confidential protected
25 health information and personally identifiable information.
26
27

1 139. The Pixel is designed such that they transmit each of the users' actions taken
2 on the webpage to a third party alongside and contemporaneously with the user initiating
3 the communication. Thus, the communication is intercepted in transit to the intended
4 recipient, Defendant and before it reaches Defendant's server.
5

6 140. As demonstrated hereinabove, Defendant violates CIPA by aiding and
7 permitting third parties to receive its users' online communications through its website
8 without their consent.
9

10 141. As a direct and proximate result of Defendant's violation of the CIPA,
11 Plaintiff and Class Members were injured and suffered damages, a loss of privacy, and loss
12 of the value of their personal information in an amount to be determined at trial.
13

14 142. By disclosing Plaintiff's and Class Members' Private Information, Defendant
15 violated Plaintiff's and Class Members' statutorily protected right to privacy.
16

17 143. As a result of the above violations and pursuant to CIPA Section 637.2,
18 Defendant is liable to each Plaintiff and Class Member for the greater of treble actual
19 damages related to their loss of privacy in an amount to be determined at trial or for
20 statutory damages in the amount of \$5,000 per violation. Section 637.2 specifically states
21 that "[it] is not a necessary prerequisite to an action pursuant to this section that the Plaintiff
22 has suffered, or be threatened with, actual damages."
23
24

25 144. Under the statute, Defendant is also liable for reasonable attorney's fees,
26 litigation costs, and injunctive and declaratory relief.
27
28

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

5 150. Plaintiff and Class Members had a reasonable expectation of privacy under
6 the circumstances, as they could not have reasonably expected that Defendant would
7 violate state and federal privacy laws.
8

9 151. Plaintiff and Class Members were not aware and could not have reasonably
10 expected that Policygenius would surreptitiously install software on its website to
11 automatically track and transmit to third parties each Plaintiff's and Class Members'
12 personally identifiable information, confidential communications and medical information.
13

14 152. Plaintiff and Class Members have an interest in: (1) precluding the
15 dissemination and/or misuse of their sensitive, confidential communications and protected
16 health information and financial information; and (2) making personal decisions and/or
17 conducting personal activities without observation, intrusion or interference, including, but
18 not limited to, the right to visit and interact with various internet sites without being
19 subjected to wiretaps without Plaintiff's and Class Members' knowledge or consent.
20
21

22 153. At all relevant times, by using software, such as Facebook's Tracking Pixel,
23 to record and communicate Plaintiff's and Class Members' personally identifiable
24
25

26 _____
27 home from unwanted communication); *Hill v. National Collegiate Athletic Assn.* (1994),
28 7 Cal.4th 1, 81, (Mosk, J., dissenting).

1 information, including unique identifiers and FIDs alongside their confidential
2 communications and medical information, Policygenius intentionally invaded Plaintiff's
3 and Class Members' privacy rights under the California Constitution.
4

5 154. Plaintiff and Class Members did not authorize Policygenius to record and
6 transmit to third parties Plaintiff's and Class Members' private communications alongside
7 their personally identifiable information and health information.
8

9 155. This invasion of privacy is serious in nature, scope, and impact because it
10 relates to Plaintiff's and Class Members' private communications, personally identifiable
11 information, and medical information. Moreover, it constitutes an egregious breach of the
12 societal norms underlying the privacy right.
13

14 156. As a result of Defendant's actions, Plaintiff and Class Members have suffered
15 harm and injury, including but not limited to an invasion of their privacy rights.
16

17 157. Plaintiff and Class Members have been damaged as a direct and proximate
18 result of Defendant's invasion of their privacy and are entitled to just compensation,
19 including monetary damages.
20

21 158. Plaintiff and Class Members seek appropriate relief for that injury, including
22 but not limited to damages that will reasonably compensate Plaintiff and Class Members
23 for the harm to their privacy interests as a result of its intrusions upon Plaintiff's and Class
24 Members' privacy.
25
26
27
28

1 159. Plaintiff and Class Members are also entitled to punitive damages resulting
2 from the malicious, willful, and intentional nature of Defendant's actions, directed at
3 injuring Plaintiff and Class Members in conscious disregard of their rights. Such damages
4 are needed to deter Defendant from engaging in such conduct in the future.
5

6 160. Plaintiff also seek such other relief as the Court may deem just and proper.
7

8 **THIRD CAUSE OF ACTION**

9 **California Common Law Invasion of Privacy – Intrusion Upon Seclusion**

10 161. Plaintiff repeats the allegations contained in the foregoing paragraphs as if
11 fully set forth herein and brings this claim individually and on behalf of the proposed Class.
12

13 162. Plaintiff and Class Members had a reasonable expectation of privacy in their
14 communications with Defendant via the Website and the communications platforms and
15 services therein.
16

17 163. Plaintiff and Class Members communicated sensitive and protected medical
18 information and personally identifiable information that they intended for only Defendant
19 to receive and that they believed Defendant would keep private.
20

21 164. Defendant's disclosure of the substance and nature of those communications
22 to third parties without the knowledge and consent of Plaintiff and Class Members is an
23 intentional intrusion on Plaintiff's and Class Members' solitude or seclusion.
24

25 165. Plaintiff and Class Members had a reasonable expectation of privacy based on
26 the sensitive nature of their communications. Plaintiff and Class Members have a general
27

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

3
4 166. Defendant's disclosure of Plaintiff and Class Member's Private Information
5 coupled with individually identifying information is highly offensive to the reasonable
6 person.

7
8 167. As a result of Defendant's actions, Plaintiff and Class Members have suffered
9 harm and injury, including but not limited to an invasion of their privacy rights.

10
11 168. Plaintiff and Class Members have been damaged as a direct and proximate
12 result of Defendant's invasion of their privacy and are entitled to just compensation,
13 including monetary damages.

14
15 169. Plaintiff and Class Members seek appropriate relief for that injury, including
16 but not limited to damages that will reasonably compensate Plaintiff and Class Members
17 for the harm to their privacy interests as a result of its intrusions upon Plaintiff's and Class
18 Members' privacy.

19
20 170. Plaintiff and Class Members are also entitled to punitive damages resulting
21 from the malicious, willful, and intentional nature of Defendant's actions, directed at
22 injuring Plaintiff and Class Members in conscious disregard of their rights. Such damages
23 are needed to deter Defendant from engaging in such conduct in the future.

24
25 171. Plaintiff also seeks such other relief as the Court may deem just and proper.
26
27

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

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

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

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

12 175. As alleged herein, Defendant’s acts, omissions, and conduct constitute
13 “business practices” within the meaning of the UCL.

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

16 177. Defendant’s acts, omissions, and conduct also violates the unfair prong of the
17 UCL because those acts, omissions, and conduct, as alleged herein, offended public policy
18 (including the aforementioned state privacy statutes and laws) and constitute immoral,
19 unethetical, oppressive, and unscrupulous activities that caused substantial injury, including
20 to Plaintiff and Class Members.
21
22
23
24
25
26
27
28

1 178. The harm caused by the Defendant’s conduct outweighs any potential benefits
2 attributable to such conduct, and there were reasonably available alternatives to further
3 Defendant’s legitimate business interests. There is no business justification for aiding and
4 enabling the interception of confidential information without adequately informing users
5 in advance that the content of their communications will be shared with Facebook.
6

7
8 179. As a result of Defendant’s violations of the UCL, Plaintiff and Class Members
9 are entitled to injunctive relief. On information and belief, this is particularly true since the
10 dissemination of Plaintiff’s and Class Members’ information is ongoing.
11

12 180. As a result of Defendant’s violations of the UCL, Plaintiff and Class Members
13 have suffered injury in fact and lost money or property. The unauthorized access to
14 Plaintiff’s and Class Members’ private and personal data has diminished the value of that
15 information. Plaintiff and the Class also derive economic value from their PII and would
16 not have provided it to Defendant or Facebook for marketing purposes in the absence of
17 consideration for that use. Thus, Defendant prevented Plaintiff and the Class from
18 capturing the full value of their Personal Information for themselves.
19
20

21 181. In the alternative to those claims seeking remedies at law, Plaintiff and Class
22 Members allege that there is no plain, adequate, and complete remedy that exists at law to
23 address Defendant’s unlawful and unfair business practices. The legal remedies available
24 to Plaintiff are inadequate because they are not “equally prompt and certain and in other
25 ways efficient” as equitable relief. *American Life Ins. Co. v. Stewart*, 300 U.S. 203, 214
26
27
28

1 (1937); *see also United States v. Bluit*, 815 F. Supp. 1314, 1317 (N.D. Cal. Oct. 6, 1992)
2 (“The mere existence’ of a possible legal remedy is not sufficient to warrant denial of
3 equitable relief.”); *Quist v. Empire Water Co.*, 2014 Cal. 646, 643 (1928) (“The mere fact
4 that there may be a remedy at law does not oust the jurisdiction of a court of equity. To
5 have this effect, the remedy must also be speedy, adequate, and efficacious to the end in
6 view ... It must reach the whole mischief and secure the whole right of the party in a perfect
7 manner at the present time and not in the future.”). Additionally, unlike damages, the
8 Court’s discretion in fashioning equitable relief is very broad and can be awarded in
9 situations where the entitlement to damages may prove difficult. *Cortez v. Purolator Air*
10 *Filtration Products Co.*, 23 Cal.4th 163, 177-180 (2000) (Restitution under the UCL can
11 be awarded “even absent individualized proof that the claimant lacked knowledge of the
12 overcharge when the transaction occurred.”). Thus, restitution would allow recovery even
13 when normal consideration associated with damages would not. *See, e.g., Fladeboe v. Am.*
14 *Isuzu Motors Inc.*, 150 Cal. App. 4th 42, 68 (2007) (noting that restitution is available even
15 in situations where damages may not be available). Furthermore, the standard for a
16 violation of the UCL “unfair” prong is different from the standard that governs legal claims.
17
18
19
20
21
22

23 182. Therefore, Plaintiff and members of the proposed Class are entitled to
24 equitable relief to restore them to a position they would have been in had Defendant not
25 engaged in unfair competition, including an order enjoining Defendant’s wrongful conduct,
26
27
28

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

3
4 **FIFTH CAUSE OF ACTION**

5 **Violation of the Electronic Communications Privacy Act**
6 **(18 U.S.C. § 2511(1)) (“ECPA”)**

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

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

10 185. 18 U.S.C. § 2520(a) provides a private right of action to any person whose
11 wire, oral, or electronic communication is intercepted.

12
13 186. A violation of the ECPA occurs where any person “intentionally intercepts,
14 endeavors to intercept, or procures any other person to intercept or endeavor to intercept,
15 any . . . electronic communication” or “intentionally discloses, or endeavors to disclose, to
16 any other person the contents of any . . . electronic communication, knowing or having
17 reason to know that the information was obtained through the [unlawful] interception of
18 a[n] . . . electronic communication” or “intentionally uses, or endeavors to use, the contents
19 of any . . . electronic communication, knowing or having reason to know that the
20 information was obtained through the [unlawful] interception of a[n] . . . electronic
21 communication.” 18 U.S.C. §§ 2511(1)(a), (c)-(d).
22
23
24
25
26
27
28

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

5 188. “Electronic communication” means “any transfer of signs, signals, writing,
6 images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire,
7 radio, electromagnetic, photoelectronic or photooptical system that affects interstate or
8 foreign commerce.” 18 U.S.C. § 2510(12).
9

10 189. “Contents” includes “any information relating to the substance, purport, or
11 meaning” of the communication at issue. 18 U.S.C. § 2510(8).
12

13 190. By utilizing and embedding the Pixel on its Website, Defendant intentionally
14 intercepted, endeavored to intercept, and procured another person to intercept, the
15 electronic communications of Plaintiff and Class Members, in violation of 18 U.S.C. §
16 2511(1)(a). Whenever Plaintiff and Class Members interacted with Defendant’s Website,
17 Defendant, through the Pixel source code it embedded and ran on its Website,
18 contemporaneously and intentionally intercepted, and endeavored to intercept Plaintiff’s
19 and Class Members’ electronic communications without authorization or consent.
20
21

22 191. By intentionally disclosing or endeavoring to disclose the electronic
23 communications of Plaintiff and Class Members to Facebook, while knowing or having
24 reason to know that the information was obtained through the interception of an electronic
25
26
27
28

1 communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. §
2 2511(1)(c).

3
4 192. By intentionally using, or endeavoring to use, the contents of the electronic
5 communications of Plaintiff and Class Members, while knowing or having reason to know
6 that the information was obtained through the interception of an electronic communication
7 in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

8
9 193. Defendant intentionally used the wire or electronic communications to
10 increase its profit margins. Defendant specifically used the Pixel to intercept and
11 disseminate Plaintiff’s and Class Members’ Private Information for financial gain.

12
13 194. Defendant was not acting under color of law to intercept Plaintiff’s and the
14 Class Members’ wire or electronic communication.

15
16 195. Plaintiff and Class Members did not authorize Defendant to acquire the
17 content of their communications for purposes of invading Plaintiff’s privacy via the Pixel
18 tracking code.

19
20 196. Any purported consent that Defendant received from Plaintiff and Class
21 Members was not valid.

22
23 197. Unauthorized Purpose – Defendant intentionally intercepted the contents of
24 Plaintiff’s and Class Members’ electronic communications for the purpose of committing
25 a tortious act in violation of the Constitution or laws of the United States or of any State –
26 namely, invasion of privacy. The ECPA provides that a “party to the communication” may
27

1 liable where a “communication is intercepted for the purpose of committing any criminal
2 or tortious act in violation of the Constitution or laws of the United States or of any State.”

3
4 18 U.S.C § 2511(2)(d).

5 198. Defendant is not a party to the communication based on its unauthorized
6 duplication and transmission of communications with Plaintiff and the Class. *In re*
7 *Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 608 (9th Cir. 2020) (an entity’s
8 simultaneous, unknown duplication and forwarding of GET requests made to a web page’s
9 server does not qualify for the party exemption, because holding otherwise “would render
10 permissible the most common methods of intrusion, allowing the exception to swallow the
11 rule”). However, even assuming Defendant is a party, Defendant’s simultaneous, unknown
12 duplication, forwarding, and interception of Plaintiff’s and Class Members’ Private
13 Information does not qualify for the party exemption.
14
15
16

17 199. Defendant is not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d)
18 on the ground that it was a participant in Plaintiff’s and the Class Members’
19 communications about their Private Information on its Website, because it used its
20 participation in these communications to improperly share Plaintiff’s and the Class
21 Members’ information with Facebook, a third-party that did not participate in these
22 communications, that Plaintiff and the Class Members did not know was receiving their
23 Private Information, and that Plaintiff and the Class Members did not consent to receive
24 this information.
25
26
27
28

1 200. As a result of Defendant’s violation of the ECPA, Plaintiff is entitled to all
2 damages available under 18 U.S.C. § 2520, including statutory damages of whichever is
3 the greater of \$100 a day for each day of violation or \$10,000, equitable or declaratory
4 relief, compensatory and punitive damages, and attorney’s fees and costs.
5

6
7 **SIXTH CAUSE OF ACTION**
8 **Unjust Enrichment/Quasi-Contract**

9 201. Plaintiff repeats the allegations contained in the foregoing paragraphs as if
10 fully set forth herein and brings this claim individually and on behalf of the proposed Class.
11

12 202. California law permits a standalone claim for unjust enrichment, allowing the
13 court to construe the cause of action as a quasi-contract claim. *E.g., Astiana v. Hain*
14 *Celestial Group, Inc.*, 783 F.3d 753, 756 (9th Cir. 2015).
15

16 203. California law recognizes a right to disgorgement of profits resulting from
17 unjust enrichment, even where an individual has not suffered a corresponding loss. *In re*
18 *Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 599 (9th Cir. 2020).
19

20 204. California law requires disgorgement of unjustly earned profits regardless of
21 whether a defendant’s actions caused a plaintiff to directly expend his or her own financial
22 resources or whether a defendant’s actions directly caused the plaintiff’s property to
23 become less valuable.
24
25
26
27
28

1 205. Under California law, a stake in unjustly earned profits exists regardless of
2 whether an individual planned to sell his or her data or whether the individual's data is
3 made less valuable.
4

5 206. Plaintiff and Class Members retain a stake in the profits garnered from their
6 Private Information because the circumstances are such that, as between Plaintiff and Class
7 Members, on the one hand, and Defendant, on the other hand, it is unjust for Defendant to
8 retain these profits.
9

10 207. By intercepting (and facilitating the interception), disclosing, and using for
11 targeted advertising Plaintiff's and Class Members' Private Information and bundled with
12 their other personal information, without their permission, Defendant generated revenues
13 and was unjustly enriched at the expense of Plaintiff and the Class. It would be inequitable
14 and unconscionable for Defendant to retain the profit, benefit, and other compensation it
15 obtained via its impermissible wiretapping and data sharing practices.
16
17

18 208. Plaintiff and the Class Members seek an order from this Court requiring
19 Defendant to disgorge all proceeds, profits, benefits, and other compensation obtained by
20 Defendant from its improper and unlawful interception (and facilitating interception),
21 disclosure, and use of their Private Information for targeted advertising.
22
23

24 209. Plaintiff and Class Members seek this equitable remedy because their legal
25 remedies are inadequate. An unjust enrichment theory provides the equitable disgorgement
26
27
28

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

3
4 **RELIEF REQUESTED**

5
6 210. Plaintiff, on behalf of herself and the proposed Class, respectfully requests
7 that the Court grant the following relief:

- 8
9 a. Determine that the claims alleged herein may be maintained as a class action
10 and issue an order certifying the Class defined above;
- 11 b. Appoint Plaintiff as the representative of the Class and counsel as Class
12 counsel;
- 13
14 c. An order enjoining Defendant from engaging in the unlawful practices and
15 illegal acts described herein;
- 16
17 d. An order awarding Plaintiff and the Class: (1) actual or statutory damages;
18 (2) punitive damages—as warranted—in an amount to be determined at trial;
19 (3) prejudgment interest on all amounts awarded; (4) equitable disgorgement
20 and injunctive relief as pleaded or as the Court may deem proper; and (5)
21 reasonable attorneys’ fees and expenses and costs of suit pursuant to Cal.
22 Code of Civil Procedure § 1021.5 and/or other applicable law; and
- 23
24 e. Other such and further relief as the Court may deem appropriate.
25
26
27
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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