

1 Mark N. Todzo (California Bar No. 168389)

2 **LEXINGTON LAW GROUP**

3 503 Divisadero Street
4 San Francisco, CA 94117
5 Telephone: 415-913-7800
6 Facsimile: 415-759-4112
7 mtodzo@lexlawgroup.com

8 Christian Levis (*pro hac vice* forthcoming)
9 Amanda Fiorilla (*pro hac vice* forthcoming)

10 **LOWEY DANNENBERG, P.C.**

11 44 South Broadway, Suite 1100
12 White Plains, NY 10601
13 Telephone: (914) 997-0500
14 Facsimile: (914) 997-0035
15 clevis@lowey.com
16 afiorilla@lowey.com

17 Anthony M. Christina (*pro hac vice* forthcoming)

18 **LOWEY DANNENBERG, P.C.**

19 One Tower Bridge
20 100 Front Street, Suite 520
21 West Conshohocken, PA 19428
22 Telephone: (215) 399-4770
23 Facsimile: (914) 997-0035
24 achristina@lowey.com

25 *Attorneys for Plaintiff Brittany Condit*

26 **UNITED STATES DISTRICT COURT**
27 **NORTHERN DISTRICT OF CALIFORNIA**
28 **SAN FRANCISCO / OAKLAND DIVISION**

29 BRITTANY CONDITI, individually and on
30 behalf of all others similarly situated,

31 Plaintiff,

32 v.

33 INSTAGRAM, LLC, a Delaware limited
34 liability company, and FACEBOOK, INC., a
35 Delaware corporation,

36 Defendants.

37 Case No.: _____

38 **CLASS ACTION COMPLAINT**

39 **JURY TRIAL DEMANDED**

1 Plaintiff Brittany Condit, individually and on behalf of all others similarly situated, asserts
2 the following against Defendants Instagram, LLC (“Instagram”) and Facebook, Inc. (“Facebook”)
3 (collectively “Defendants”), based upon personal knowledge, where applicable, information and
4 belief, and the investigation of counsel.

5 **SUMMARY OF ALLEGATIONS**

6 1. Instagram is a popular social media platform, wholly owned by Facebook, with
7 approximately one billion annual active users.

8 2. Instagram’s focus as a social media platform is based on allowing users to share
9 photographs and videos with one another. Originally, users were only able to post photographs or
10 videos to their Instagram “Feed,” which is a permanent collection of users’ content that others can
11 interact with by viewing, commenting, or liking. In August 2016, Instagram launched “Stories,” a
12 feature where users can post photographs or videos that disappear from view within a 24-hour
13 period.

14 3. As a social media platform that allows users to post photographs and videos,
15 Instagram has access to a user’s smartphone camera for the limited purpose of allowing users to
16 directly take a photograph or video and then post that content to its platform.

17 4. Instagram claims to only access users’ smartphone cameras with user permission,
18 such as when a user is interacting with the Instagram application’s (also referred to as an “app”)
19 camera feature.

20 5. For example, Instagram recently released a statement saying “[Instagram] only
21 access[es] your camera when you tell us to—for example, when you swipe from Feed to Camera.”
22 Instagram claims when its camera feature is not used, it does not access users’ smartphone cameras.¹

23 6. However, Instagram does more than it claims. Instagram is constantly accessing
24 users’ smartphone camera feature while the app is open and monitors users without permission, i.e.,
25

26 ¹ Filipe Esposito, *Instagram Promises to Fix Bug After Being Exposed By Always Accessing*
27 *the Camera on iOS 14*, 9TO5MAC, (July 25, 2020), [https://9to5mac.com/2020/07/25/instagram-](https://9to5mac.com/2020/07/25/instagram-promises-to-fix-bug-after-being-exposed-by-always-accessing-the-camera-on-ios-14/)
28 [promises-to-fix-bug-after-being-exposed-by-always-accessing-the-camera-on-ios-14/](https://9to5mac.com/2020/07/25/instagram-promises-to-fix-bug-after-being-exposed-by-always-accessing-the-camera-on-ios-14/).

1 when users are not interacting with Instagram’s camera feature.

2 7. This access goes beyond the services that Instagram promises to provide. Instagram
3 has no legitimate reason for accessing users’ smartphone cameras when they are not using the
4 Instagram camera feature.

5 8. By doing so, Defendants have been able to monitor users’ most intimate moments,
6 including those in the privacy of their own homes, in addition to collecting valuable insight and
7 market research on its users.

8 9. Defendants engage in this conduct for one main reason: to collect lucrative and
9 valuable data on its users that it would not otherwise have access to. By obtaining extremely private
10 and intimate personal data on their users, including in the privacy of their own homes, Defendants
11 are able to increase their advertising revenue by targeting users more than ever before. For example,
12 Defendants are able to see in-real time how users respond to advertisements on Instagram, providing
13 extremely valuable information to its advertisers.

14 10. The full extent and scope of Defendants’ conduct is only just beginning to come to
15 light as a result of an update to the Apple Inc.’s (“Apple”) iPhone operating system, which provides
16 notice to consumers when third parties are accessing their camera and microphone or collecting their
17 data. The update to iPhone’s operating system was only made available to developers on June 22,
18 2020, and to the general public on July 9, 2020.

19 11. Defendants’ conduct constitutes an egregious violation of Plaintiff’s and Class
20 members’ privacy rights, as established through California’s privacy laws. In addition, Defendants’
21 actions constitute violations of the common law as well as several state and federal laws.

22 **JURISDICTION AND VENUE**

23 12. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C
24 § 1332(d), because the amount in controversy for the Class exceeds \$5,000,000 exclusive of interest
25 and costs, there are more than 100 putative class members, and minimal diversity exists because a
26 significant portion of putative class members are citizens of a state different from the citizenship of
27 Defendants.

1 26. Due to Instagram’s ever-increasing user base, Instagram began to garner attention
2 from larger technology companies, such as Facebook, Twitter, and Benchmark Capital. After
3 denying an offer to be bought-out by Twitter, Facebook eventually acquired Instagram for one
4 billion dollars in 2012.

5 27. Instagram has become a large part of Facebook’s overall revenue stream. For
6 example, in 2019, Instagram brought in over \$20 billion in advertising revenue, accounting for more
7 than a quarter of Facebook’s total revenue that year.

8 28. With access to so many users, Defendants have claimed to value full transparency
9 and to respect user’s privacy. For example, Mark Zuckerberg claimed in an open letter while
10 “Facebook and Instagram have helped people connect with friends, communities, and interests . . .
11 people increasingly also want to connect privately.”⁴

12 29. To that end, Mark Zuckerberg promised to build a “privacy-focused platform” and
13 claimed to have “worked hard to build privacy into all our products, including those for public
14 sharing.”⁵ These empty promises have not been fulfilled.

15 30. As alleged herein, Defendants took advantage of Plaintiff and Class members by
16 secretly accessing their smartphone cameras to monitor users beyond the scope of any services that
17 Defendants agreed to provide, i.e., when users were not interacting with the Instagram camera
18 feature.

19 31. As a result, Defendants have been able to secretly spy on users, including Plaintiff
20 and Class members, during intimate moments and in private places, such as their bedroom, to gather
21 lucrative data to increase its advertising revenue.

22 **II. Instagram Watches Users Through Their Smartphone Cameras**

23 32. On July 25, 2020, reports emerged for the first time that Instagram was secretly
24

25 ⁴ Mark Zuckerberg, *A Privacy-Focused Vision for Social Networking*, FACEBOOK, (Mar. 6,
26 2019), <https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/>.

27 ⁵ *Id.*
28

1 accessing and spying on users through their smartphone camera without their consent.

2 33. Users were able to discover that Instagram was secretly monitoring them through a
3 new update to Apple’s smartphone operating system.

4 34. Apple’s latest operating system (“iOS”) update has been declared a “game-changer”
5 by *Forbes*, specifically because it allows users to see exactly how companies access and use their
6 personal information.⁶

7 35. Apple released iOS 14 to developers on June 22, 2020, and the general public on July
8 9, 2020. Among other things, the update allows users to see which applications are accessing their
9 camera or microphone, which reportedly “exposed” Instagram’s conduct.

10 36. The update informs users by a green “camera on” indicator that companies, such as
11 Instagram, are monitoring them through their camera. Instagram users were notified by the green
12 “camera on” indicator that Instagram was accessing, and monitoring them through, their cameras
13 while they were not using Instagram’s camera feature and for reasons beyond any “service” that
14 Instagram claims to provide.

15 37. Instagram is not the only company who has been caught spying on users as a result
16 of Apple’s latest update. TikTok, LinkedIn, and Reddit all face scrutiny for copying user’s clipboard
17 information after Apple began providing similar notifications whenever this occurred.

18 38. In a statement, Instagram claimed to “only access your camera when you tell us to—
19 for example when you swipe from Feed to Camera.”⁷ Instagram’s data policy provides similar
20 assurances about the services it does, and does not, provide, and when it collects information and
21 data.

22 39. Instagram’s data policy states that it can collect information, such as “what you see
23

24 ⁶ Davey Winder, *Apple iOS 14 Exposes Microsoft’s LinkedIn App Reading Clipboard Data*,
25 FORBES, (July 4, 2020), <https://www.forbes.com/sites/daveywinder/2020/07/04/apple-ios-14-catches-microsofts-linkedin-spying-on-clipboard-tiktok-apps-privacy-iphone-ipad-macbook/#10c5380f5896>.

26 ⁷ Kim Lyons, *An Instagram bug showed a ‘camera on’ indicator for iOS 14 devices even*
27 *when users weren’t taking photos*, THE VERGE, (July 25, 2020),
28 <https://www.theverge.com/2020/7/25/21338151/instagram-bug-camera-privacy-ios14-apple>.

1 through features we provide, such as our camera, so [Instagram] can do things like suggest masks
2 and filters that you might like, or give you tips on using camera formats.”⁸ Instagram discloses that
3 it collects “information about how you use features like our camera.”⁹

4 40. However, nowhere in Instagram’s data policy does it disclose that, when users are
5 not using its camera feature, Instagram is secretly accessing users’ smartphone camera to monitor
6 individuals, such as Plaintiff. This is beyond the scope of services that Instagram provides and
7 Instagram has no legitimate reason to access users’ smartphone cameras while they are not
8 interacting with Instagram’s camera feature.

9 41. Instagram’s conduct in secretly monitoring users constitutes an egregious violation
10 of their privacy rights, especially because many users, including Plaintiff, were monitored in the
11 privacy of their own home.

12 42. Defendants abused their ability to access users’ smartphone cameras, and committed
13 egregious privacy violations, for one specific reason: to increase their advertising revenue. By
14 obtaining extremely private and intimate personal data on their users, including in the privacy of
15 their own home, Defendants are able to target users more than ever before.

16 43. Facebook has acknowledged the impact that Apple’s update to its operating system
17 will pose to its potential advertising revenue, which it earns through its extensive data collection.
18 Since Apple began rolling out its latest operating system update, which gives users unprecedented
19 control over their own data, Facebook has begun meeting with its most notable advertising partners
20 to discuss its potential repercussions.

21 44. Apple’s Chief Financial Officer, David Wehner, told *CNBC* that it believes Apple’s
22 update will “make it harder for app developers and others to grow ads on Facebook and
23
24
25

26 ⁸ *Data Policy*, INSTAGRAM,
27 https://help.instagram.com/519522125107875?helpref=page_content (last visited July 30, 2020).

28 ⁹ *Id.*

1 elsewhere.”¹⁰ Considering that Instagram’s advertising revenue constitutes a significant part of
2 Facebook’s overall revenue, it’s not surprising the lengths they would go in pursuit of obtaining
3 users’ data for advertising purposes, regardless of the privacy violations they commit in the process.

4 **III. Instagram Does Not Obtain Consent or Disclose That it Monitors Users**

5 45. Instagram does not obtain users’ consent to access their smartphone cameras while
6 users are not interacting with Instagram’s camera feature.

7 46. Nowhere in Instagram’s data policy does it disclose that it (1) accesses users’
8 smartphone camera while the Instagram camera feature is not in use; or (2) obtain consent to do so.

9 47. Nor could it. Instagram has no legitimate purpose for accessing users’ smartphone
10 cameras while they are not using Instagram’s services, i.e., accessing Instagram’s camera feature.
11 Since this is not a part of any services that Instagram provides, and Instagram claims to “only access
12 your camera when you tell us to,” users could in no way consent to this conduct.

13 48. Rather, Instagram has claimed this was simply a “mistake” because of “a bug in iOS
14 14 Beta that [] indicates that some people are using the camera when they aren’t.”¹¹ iOS is Apple’s
15 proprietary operating system. Apple has not acknowledged that there is any “bug” in its software
16 that would affect the operation of Instagram.

17 49. Tellingly, Facebook came under similar scrutiny for also accessing users’
18 smartphone cameras last year. Users reported that the camera for “Facebook Stories,” similar to
19 Instagram Stories, would open in the background while they were watching videos or viewing
20 pictures on Facebook.

21 50. Similar to Instagram, Facebook claimed this was a “bug” and entirely inadvertent.¹²

22 _____
23 ¹⁰ Filipe Esposito, *Facebook raises concerns that iOS 14 could harm its ad business*,
24 9TO5MAC, (July 30, 2020), <https://9to5mac.com/2020/07/30/facebook-raises-concerns-that-ios-14-could-harm-its-ad-business/>.

25 ¹¹ Kim Lyons, *supra* note 9.

26 ¹² Jay Peters, *Facebook’s iOS app might be opening the camera in the background without*
27 *your knowledge*, THE VERGE (Nov. 12, 2019),
28 <https://www.theverge.com/2019/11/12/20961332/facebooks-ios-app-reportedly-camera-background-security>.

1 Notably, neither company came forward about these “bugs” until after users discovered what they
2 were doing through Apple’s update to its operating system.

3 51. As Instagram denies that it monitors users while its camera function is not in use,
4 this is not listed as one of the services Instagram promises to provide its users nor is it listed as one
5 of the ways Instagram collects user data.

6 52. Similarly, since Instagram does not disclose this practice, there is no way for users
7 to provide consent to be monitored through their smartphone camera while they are not engaging
8 with Instagram’s camera function.

9 **IV. Instagram’s Conduct Violates the California Consumer Privacy Act**

10 53. The California Consumer Privacy Act (“CCPA”) protects consumers’ personal
11 information from collection and use by businesses without providing proper notice and obtaining
12 consent.

13 54. Instagram and Facebook are required to comply with the CCPA because they
14 individually earn more than \$25 million in annual gross revenue. Additionally, the CCPA applies to
15 Defendants because they buy, sell, receive, or share, for commercial purposes, the personal
16 information of more than 50,000 consumers, households, or devices.

17 55. The CCPA requires that a business who collects consumer’s personal information,
18 such as Defendants, disclose either “at or before the point of collection . . . the categories of personal
19 information to be collected and the purposes for which the categories of personal information shall
20 be used. *See* Cal. Civ Code § 1798.100(b).

21 56. Furthermore, “[a] business shall not collect additional categories of personal
22 information or use personal information collected for additional purposes without providing the
23 consumer with notice consistent with this section.” *See id.*

24 57. Defendants violated the CCPA by failing to disclose that it monitors users through
25 their smartphone camera, while it’s not in use, to collect personal information. Instagram only
26
27
28

1 discloses that it collects “information about how you use features like our camera.”¹³ Since users
 2 were not interacting with Instagram’s camera feature at the time they were monitored, and
 3 Defendants failed to disclose its conduct, Defendants violated the CCPA.

4 **V. Instagram Users Have a Reasonable Expectation of Privacy**

5 58. Plaintiff and Class members have a reasonable expectation of privacy not to be
 6 watched and monitored without their permission. This expectation of privacy is deeply enshrined in
 7 California’s Constitution.

8 59. Article I, section 1 of the California Constitution provides: “All people are by nature
 9 free and independent and have inalienable rights. Among these are enjoying and defending life and
 10 liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety,
 11 happiness, *and privacy*.” Art. I., Sec. 1, Cal. Const. [Emphasis added].

12 60. The phrase “*and privacy*” was added in 1972 after voters approved a proposed
 13 legislative constitutional amendment designated as Proposition 11. Critically, the argument in favor
 14 of Proposition 11 reveals that the legislative intent was to curb businesses’ control over the
 15 unauthorized collection and use of consumers’ personal information, stating in relevant part:

16 The right of privacy is the right to be left alone . . . It prevents government and
 17 business interests from collecting and stockpiling unnecessary information about us
 18 and from misusing information gathered for one purpose in order to serve other
 purposes or to embarrass us.

19 **Fundamental to our privacy is the ability to control circulation of personal**
 20 **information.** This is essential to social relationships and personal freedom. The
 21 proliferation of government and business records over which we have no control
 limits our ability to control our personal lives. Often we do not know that these
 records even exist and we are certainly unable to determine who has access to them.¹⁴

22 (Emphasis added).

23 61. Consistent with this language, an abundance of studies examining the collection of
 24 consumers’ personal data confirms that the surreptitious monitoring of millions of individuals, as

25 ¹³ *Data Policy*, INSTAGRAM,
 26 https://help.instagram.com/519522125107875?helpref=page_content (last visited Aug. 19, 2020).

27 ¹⁴ Ballot Pamp., Proposed Amends. to Cal. Const. with arguments to voters, Gen. Elec. (Nov.
 28 7, 1972) at 27.

1 Instagram has done here, violates expectations of privacy that have been established as general
 2 social norms. Privacy polls and studies uniformly show that the overwhelming majority of
 3 Americans consider one of the most important privacy rights to be the need for an individual's
 4 affirmative consent before a company collects and shares its customers' personal data.

5 62. For example, a recent study by *Consumer Reports* shows that 92% of Americans
 6 believe that internet companies and websites should be required to obtain consent before selling or
 7 sharing their data and the same percentage believe internet companies and websites should be
 8 required to provide consumers with a complete list of the data that has been collected about them.¹⁵

9 63. Moreover, according to a study by *Pew Research*, a majority of Americans,
 10 approximately 79%, are concerned about how data is collected about them by companies. *Pew*
 11 *Research* also found that 85% of Americans are concerned about the personal information social
 12 media sites know about them.

13 64. Instagram has failed to obtain adequate consent to access users' smartphone camera
 14 while users are not interacting with Instagram's camera feature and has chosen to secretly monitor
 15 users without their permission. This constitutes a violation of Plaintiff's and Class members' privacy
 16 interests, including those explicitly enshrined in the California Constitution.

17 **VI. Facebook's and Instagram's Shared History of Privacy Violations**

18 65. Since its inception in 2004, Facebook's core business model has been monetizing
 19 user information. As the Federal Trade Commission ("FTC") noted in a 2019 complaint against
 20 Facebook, "substantially all of Facebook's \$55.8 billion in 2018 revenues came from advertising."¹⁶
 21 It is therefore no surprise that Facebook's fortune rises only at the expense of its users, as evidenced
 22 by Facebook's long history of data abuse and privacy violations.

23 66. For example, back in 2007, when Facebook launched "Facebook Beacon," users
 24 were unaware that their online activity was tracked, and that the privacy settings originally did not
 25

26 ¹⁵ *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey*
 27 *Finds*, CONSUMER REPORTS (May 11, 2017), <https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/>.

28 ¹⁶ *United States v. Facebook, Inc.*, Case No. 19-cv-2184.

1 allow users to opt-out. As a result of widespread criticism, Facebook Beacon was eventually shut
2 down.

3 67. Just two short years later, Facebook made controversial modifications to its Terms
4 of Service, which allowed Facebook to use anything a user uploaded to its site for any purpose, at
5 any time, even after the user ceased to use Facebook. The Terms of Service also failed to provide
6 anyway for users to completely delete their accounts. Under immense public pressure, Facebook
7 eventually returned to its previous Terms of Service.

8 68. In November of 2011, Facebook agreed to settle FTC charges that it repeatedly failed
9 to keep promises concerning user privacy, including claims that Facebook promised users it would
10 not share personal information with advertisers. Jon Leibowitz, Chairman of the FTC, warned
11 “Facebook is obligated to keep the promises about privacy that it makes to its hundreds of millions
12 of users . . . Facebook’s innovation does not have to come at the expense of consumer privacy.”¹⁷

13 69. The resulting Consent Order prohibited Facebook from misrepresenting the extent to
14 which consumers can control the privacy of their information, the steps that consumers must take to
15 implement such controls, and the extent to which Facebook makes user information accessible to
16 third parties.¹⁸

17 70. But this was not the last time Facebook abused users’ data. In 2015, a journalist for
18 *The Guardian* reported that Cambridge Analytica was using data harvested from millions of users’
19 Facebook accounts mostly without user consent.

20 71. In 2018, Facebook testified before Congress that Cambridge Analytica may have
21 harvested the data of up to 87 million users in connection with the 2016 election. This led to yet
22 another FTC investigation in 2019 into Facebook’s data collection and privacy practices, resulting
23 in a record-breaking five billion dollar settlement.

24 72. Acknowledging that Facebook does not “currently have a strong reputation for
25 building privacy protective services,” Mark Zuckerberg promised to build a “privacy-focused

26 ¹⁷ *Id.*

27 ¹⁸ Fed. Trade Comm’n., *In re Facebook*, Decision and Order, FTC File No. 092 3184 (Jul. 27, 2012)

1 platform” and assured users that it has “worked hard to build privacy into all our products, including
2 those for public sharing.”¹⁹

3 73. Despite these promises, Facebook has continued to fail to live up to its promises. In
4 April 2019, a cybersecurity firm found that millions of Facebook records were made public on
5 Amazon’s cloud computing server, which were “accessible and downloadable for anyone who could
6 find them online.”²⁰

7 74. Even more significant, Facebook has come under scrutiny for nearly the same exact
8 thing Instagram is alleged to have done here. In November of 2019, *The Verge* reported that
9 “Facebook’s iOS app appears to be activating the camera in the background of the app in some
10 situations without a user’s knowledge.”²¹ Like here, Facebook’s conduct was only revealed by users
11 with iPhones running a new version of Apple’s operating software. Tellingly, Facebook, like
12 Instagram here, claimed that this was merely a “bug” that they would fix.

13 75. Instagram has followed a similar path of repeated privacy violations as its parent
14 company. In 2012, shortly after being acquired by Facebook, Instagram announced sweeping
15 changes to its Terms of Service disclosing that “a business or other entity may pay” Instagram for
16 the use of a users’ images “without any compensation [to the user].”²² The changes also allowed
17 Instagram to disclose user data to Facebook and third-party advertisers. Even worse, Instagram
18 proposed that parents of minors implicitly consented to the use of their children’s images for

19 _____
20 ¹⁹ Mark Zuckerberg, *A Privacy-Focused Vision for Social Networking*, FACEBOOK, (Mar. 6,
21 2019), <https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/>.

22 ²⁰ Sarah Frier, Matt Day & Josh Eidelson, *Hundreds of Millions of Facebook User Records*
23 *Exposed on Amazon Cloud Servers*, LA TIMES, (April 3, 2019),
<https://www.latimes.com/business/la-fi-tn-facebook-user-data-amazon-web-services-privacy-20190403-story.html>.

24 ²¹ Jay Peters, *Facebook’s iOS app might be opening the camera in the background without*
25 *your knowledge*, THE VERGE (Nov. 12, 2019),
26 <https://www.theverge.com/2019/11/12/20961332/facebooks-ios-app-reportedly-camera-background-security>.

27 ²² Doug Gross, *Instagram Backtracks After User Privacy Revolt*, CNN (Dec. 19, 2012),
28 <https://www.cnn.com/2012/12/18/tech/social-media/instagram-terms-users/index.html>.

1 advertising purposes by posting them to Instagram. Amidst widespread protests and boycotts,
2 Instagram claimed they would withdraw the proposed changes.

3 76. In February 2020, reports emerged that Instagram retained users' pictures and private
4 messages on their servers long after users manually deleted them. Even though Instagram claimed
5 that it typically retains pictures and private messages for about 90 days after a user deletes them, in
6 some instances Instagram kept this data for as long as a year. Instagram was alerted to the issue in
7 October 2019 and took nearly *eight months* to resolve the issue.

8 77. It is therefore not surprising that Defendants have once again abused its access to
9 users to commit egregious privacy violations by monitoring users through their smartphone
10 cameras, while they are not interacting with the Instagram camera feature, including during intimate
11 and private moments in one's own home.

12 TOLLING OF THE STATUTE OF LIMITATIONS

13 78. The applicable statutes of limitations have been tolled by Instagram's knowing and
14 active concealment and denial of the facts alleged herein, namely its practice of spying and
15 monitoring users through their smartphone camera, and collecting and otherwise misusing data
16 gathered from Plaintiff's and Class members' private and intimate moments. Plaintiff and Class
17 members could not have reasonably discovered the truth about Instagram's practices until shortly
18 before this class action litigation was commenced.

19 79. As alleged in detail herein, Instagram expressly and impliedly assured consumers
20 that it would only collect information about how Plaintiff and Class members "use features like
21 [their] camera."²³ At no point in time did Instagram disclose that it would access and collect
22 information from users through their smartphone camera while it's features are *not* in use.
23 Instagram's public assurances and policies deny that Instagram engages in the practices described
24 herein.

25
26 _____
27 ²³ *Data Policy*, INSTAGRAM,
28 https://help.instagram.com/519522125107875?helpref=page_content (last visited Aug. 19, 2020).

1 80. Furthermore, Plaintiff and Class members have a reasonable expectation of privacy
2 not to be secretly watched and monitored regardless of Instagram’s express assurances. This
3 expectation is particularly heightened where, as here, such communication occurs within one’s
4 home, which is a zone of privacy uniformly recognized by state and federal privacy laws.

5 81. Thus, based on Instagram’s representations and Plaintiff’s and Class members’
6 expectations of privacy, Plaintiff and Class members would not have been able to uncover the facts
7 underlying their claims prior to the update to Apple’s iOS, which was only released to developers
8 on June 22, 2020, and made public on July 9, 2020, that exposed Instagram’s practice of spying and
9 monitoring users through their smartphone camera, and collecting and otherwise misusing their data.
10 This is because all relevant facts were in the possession of Instagram who actively concealed their
11 existence.

12 **CLASS ACTION ALLEGATIONS**

13 82. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23
14 individually and on behalf of the following Class:

15 All Instagram users whose smartphone cameras were accessed by Instagram without
16 their consent from 2010 through the present (the “Class Period”).²⁴

17 83. Excluded from each Class are: (1) any Judge or Magistrate presiding over this action
18 and any members of their families; (2) Defendants, Defendants’ subsidiaries, parents, successors,
19 predecessors, and any entity in which Defendants or its parent has a controlling interest and their
20 current or former employees, officers, and directors; (3) persons who properly execute and file a
21 timely request for exclusion from the Class; (4) persons whose claims in this matter have been
22 finally adjudicated on the merits or otherwise released; (5) Plaintiff’s counsel and Defendants’
23 counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

24 84. **Ascertainability:** Membership of the Class is defined based on objective criteria,
25 and individual members will be identifiable from Defendants’ records.

26 _____

27 ²⁴ Plaintiff has defined the Class based on currently available information and hereby reserves
28 the right to amend the definition of the Class, including, without limitation, the Class Period

1 85. **Numerosity:** The exact number of members of the Class is unknown and unavailable
2 to Plaintiff at this time, but individual joinder in this case is impracticable. The Class likely consists
3 of millions of individuals, and the members can be identified through Defendants’ records.

4 86. **Predominant Common Questions:** The Class’s claims present common questions
5 of law and fact, and those questions predominate over any questions that may affect individual Class
6 members. Common questions for the Class include, but are not limited to, the following:

- 7 a. Whether Defendants violated Plaintiff’s and Class members’ privacy rights;
- 8 b. Whether Defendants’ acts and practices complained of herein amount to
9 egregious breaches of social norms;
- 10 c. Whether Defendants’ conduct was unlawful;
- 11 d. Whether Defendants’ conduct was unfair;
- 12 e. Whether Defendants’ conduct was fraudulent;
- 13 f. Whether Plaintiff and Class members are entitled to equitable relief,
14 including but not limited to, injunctive relief, restitution, and disgorgement; and,
- 15 g. Whether Plaintiff and Class members are entitled to actual, statutory, punitive
16 or other forms of damages, and other monetary relief.

17 87. **Typicality:** Plaintiff’s claims are typical of the claims of the other members of the
18 proposed Class. Defendants’ conduct that gave rise to Plaintiff’s claims and the members of the
19 Class is the same for all members of the Class.

20 88. **Adequate Representation:** Plaintiff has and will continue to fairly and adequately
21 represent and protect the interests of the Class. Plaintiff has retained counsel competent and
22 experienced in complex litigation and class actions, including privacy violations. Plaintiff has no
23 interest that is antagonistic to those of the Class, and Defendants have no defenses unique to any
24 Plaintiff. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of
25 the members of the Class, and they have the resources to do so. Neither Plaintiff nor her counsel
26 have any interest adverse to those of the other members of the Class.

27 89. **Substantial Benefits:** This class action is appropriate for certification because class
28

1 proceedings are superior to other available methods for the fair and efficient adjudication of this
2 controversy and joinder of all members of the Class is impracticable. This proposed class action
3 presents fewer management difficulties than individual litigation, and provides the benefits of single
4 adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment
5 will create economies of time, effort, and expense and promote uniform decision-making.

6 90. Plaintiff reserves the right to revise the foregoing class allegations and definitions
7 based on facts learned and legal developments following additional investigation, discovery, or
8 otherwise.

9 **CALIFORNIA LAW APPLIES TO THE ENTIRE CLASS**

10 91. California's substantive laws apply to every member of the Class, regardless of
11 where in the United States the Class member resides.

12 92. Instagram's Terms of Service states "[w]hen you create an Instagram account or use
13 Instagram, you agree to these terms." The Terms of Service specifically state that claims "will be
14 resolved exclusively in the U.S. District Court for the Northern District of California . . . You also
15 agree to submit to the personal jurisdiction of [this] court[] for the purpose of litigating any such
16 claim," and "[t]he laws of the State of California, to the extent not preempted by or inconsistent with
17 federal law, will govern these Terms and any claim, without regard to conflict of law provisions."²⁵

18 93. Facebook's Terms of Service states that "you agree that [any claim] will be resolved
19 exclusively in the U.S. District Court for the Northern District of California . . . You also agree to
20 submit to the personal jurisdiction of [this] court[] for the purpose of litigating any such claim, and
21 that the laws of the State of California will govern these Terms and any claim, without regard to
22 conflict of law provisions."²⁶

23 94. By choosing California law for the resolution of disputes, Defendants concede that
24 is it appropriate for this Court to apply California law to this action.

25 _____
26 ²⁵ *Terms of Use*, INSTAGRAM, <https://help.instagram.com/581066165581870/> (last visited Aug. 11,
27 2020).

28 ²⁶ *Terms of Service*, FACEBOOK, <https://www.facebook.com/terms.php> (last visited Aug. 11, 2020).

1 95. Further, California’s substantive laws may be constitutionally applied to the claims
2 of Plaintiff and the Class under the Due Process Clause, 14th Amend. § 1, and the Full Faith and
3 Credit Clause, Art. IV § 1 of the U.S. Constitution. California has significant contacts, or significant
4 aggregation of contacts, to the claims asserted by Plaintiff and all Class members, thereby creating
5 state interests that ensure that the choice of California state law is not arbitrary or unfair.

6 96. Defendants’ United States headquarters and principal place of business is located in
7 California. Defendants also own property and conduct substantial business in California, and
8 therefore California has an interest in regulating Defendants’ conduct under its laws. Defendants’
9 decision to reside in California and avail itself of California’s laws, and to engage in the challenged
10 conduct from and emanating out of California, renders the application of California law to the claims
11 herein constitutionally permissible.

12 97. California is also the state from which Defendants’ alleged misconduct emanated.
13 This conduct similarly injured and affected Plaintiff and all other Class members.

14 98. The application of California laws to the Class is also appropriate under California’s
15 choice of law rules because California has significant contacts to the claims of Plaintiff and the
16 proposed Class, and California has a greater interest in applying its laws here than any other
17 interested state.

18 **CLAIMS FOR RELIEF**

19 **FIRST CLAIM FOR RELIEF**

20 **Common Law Invasion of Privacy – Intrusion Upon Seclusion**
21 **(On Behalf of Plaintiff and the Class)**

22 99. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with
23 the same force and effect as if fully restated herein.

24 100. A plaintiff asserting claims for intrusion upon seclusion must plead (1) that the
25 defendant intentionally intruded into a matter as to which plaintiff had a reasonable expectation of
26 privacy; and (2) that the intrusion was highly offensive to a reasonable person.

27 101. Defendants intruded upon Plaintiff’s and Class members’ seclusion by (1) secretly
28 monitoring users through their smartphone cameras, including in their own home and during private

1 and intimate moments, in which they had a reasonable expectation of privacy; and (2) in a manner
2 that was highly offensive to Plaintiff and Class members, would be highly offensive to a reasonable
3 person, and was an egregious violation of social norms.

4 102. Defendants' business practice of secretly monitoring Plaintiff and Class members
5 through their smartphone camera without their consent constituted an intentional intrusion upon
6 Plaintiff's and Class members' solitude or seclusion in that Defendants effectively placed
7 themselves in the middle of conversations and intimate moments to which it was not invited,
8 welcomed, or authorized.

9 103. The surreptitious monitoring and spying on millions of individuals was highly
10 offensive because it violated expectations of privacy that have been established by general social
11 norms. Privacy polls and studies consistently show that the overwhelming majority of Americans
12 believe one of the most important privacy rights is the need for an individual's affirmative consent
13 before personal information is shared. For example, one study by *Pew Research* found that 93% of
14 Americans believe its important to be in control of who can get information about them.

15 104. Defendants' conduct would be highly offensive to a reasonable person in that it
16 violated federal and state laws designed to protect individual privacy, in addition to social norms.

17 105. Defendants intentionally engaged in the misconduct alleged herein for its own
18 financial benefit, such as collecting valuable (and private) sensitive information on its users for
19 marketing and advertisement purposes.

20 106. As a result of Defendants' actions, Plaintiff and Class members have suffered harm
21 and injury, including, but not limited to, an invasion of their privacy rights.

22 107. Unwanted monitoring and collection of sensitive personal information in violation
23 of the law or social norms is actionable under California law.

24 108. Plaintiff and Class members have been damaged as a direct and proximate result of
25 Defendants' invasion of their privacy and are entitled to just compensation.

26 109. Plaintiff and Class members are entitled to appropriate relief, including
27 compensatory damages for the harm to their privacy and dignitary interests, loss of valuable rights
28

1 and protections, heightened risk of future invasions of privacy, and mental and emotional distress.

2 110. Plaintiff and Class members are entitled to an order requiring Defendants to disgorge
3 profits or other benefits that Defendants acquired as a result of its invasions of privacy.

4 111. Plaintiff and Class members are entitled to punitive damages resulting from the
5 malicious, willful and intentional nature of Defendants’ actions, directed at injuring Plaintiff and
6 Class members in conscious disregard of their rights. Such damages are needed to deter Defendants
7 from engaging in such conduct in the future.

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

9 **SECOND CLAIM FOR RELIEF**
10 **Violation of Cal. Civ. Code § 1709**
11 **(On Behalf of Plaintiff and the Class)**

12 113. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with
13 the same force and effect as if fully restated herein.

14 114. California Civil Code § 1709 provides that “[o]ne who willfully deceives another
15 with intent to induce him to alter his position to his injury or risk, is liable for any damage which he
16 thereby suffers.” A defendant violates § 1709 if (i) it had a duty to disclose a material fact to the
17 plaintiff; (ii) it intentionally concealed that fact with intent to defraud; (iii) plaintiff was unaware of
18 that fact (and would have acted differently if he were aware), and (iv) plaintiff sustained some
19 damage as a result.

20 115. California Civil Code § 1710 defines “deceit” as “1. [t]he suggestion, as a fact, of
21 that which is not true, by one who does not believe it to be true; 2. [t]he assertion, as a fact, of that
22 which is not true, by one who has no reasonable ground for believing it to be true; 3. [t]he
23 suppression of a fact, by one who is bound to disclose it, or who gives information of other facts
24 which are likely to mislead for want of communication of that fact; or, 4. [a] promise, made without
25 any intention of performing it.”

26 116. Defendants violated § 1709 by failing to disclose and/or omitting that it accessed and
27 monitored users through their smartphone camera while users were not interacting with the
28 Instagram camera feature.

1 117. Defendants had a duty to disclose this information because the way in which
2 Defendants' access and use the camera within Instagram is in their exclusive control.

3 118. This information was material because Plaintiff and Class members would not have
4 used Instagram if they had known they were secretly monitored by Defendants.

5 119. Plaintiff and Class members had no way of discovering that Defendants access users'
6 cameras when they are not activated by the individual prior to the update to iOS that revealed this
7 material information.

8 120. Additionally, Defendants' partial representations about when they accessed users'
9 cameras created an obligation to disclose the true nature of that interaction. Specifically, Defendants
10 represented to Plaintiff and Class members in their Data Policy that they would only access and
11 collect camera data while users were engaging with the Instagram camera feature. This omitted that
12 Defendants also access the user's camera when they are in other parts of the app, such as scrolling
13 through their feed. Defendant's failure to disclose this information to Plaintiff and Class members
14 concealed the full extent to which they access users' smartphone cameras, including when the
15 camera is not activated by the user.

16 121. Defendants actively concealed that they would access Plaintiff's and Class members'
17 smartphone cameras while the Instagram camera feature was not in use with the intent to induce
18 Plaintiff and Class members to alter their position to their injury or risk; namely, to download and/or
19 use Instagram.

20 122. Defendants willfully engaged in these acts of deceit so that they could have access
21 to, and monitor, Plaintiff's and Class members' sensitive and confidential activity for their own
22 personal benefit, including collecting valuable marketing information.

23 123. Plaintiffs suffered injury as a direct result of Defendants' deceit, including an
24 invasion of their right to privacy. Additionally, Plaintiffs were injured because Defendants obtained
25 their personal and highly confidential information by accessing their smartphone camera without
26 permission. This information is highly valuable and conferred a direct benefit to Defendants, such
27 as boosting their advertisement revenue, to Plaintiffs detriment.
28

1 124. As a result, Plaintiff and Class members seek recovery of their resulting damages,
2 including economic damages, restitution, and disgorgement, as well as punitive damages and such
3 other relief as the Court may deem just and proper.

4 **THIRD CLAIM FOR RELIEF**
5 **Violation of California Unfair Competition Law (“UCL”)**
6 **Cal. Civ. Code § 17200, *et seq.***
7 **(On Behalf of Plaintiff and the Class)**

8 125. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with
9 the same force and effect as if fully restated herein.

10 126. Defendants’ conduct as alleged herein constitutes unlawful, unfair, and/or fraudulent
11 business acts or practices as prohibited by the UCL.

12 127. Defendants engaged in business acts and practices deemed “unlawful” under the
13 UCL, because, as alleged above, Defendants unlawfully monitored and spied on Plaintiff and Class
14 members through their smartphone camera without consent in violation of the California common
15 law, California Constitution, the Federal Wiretap Act, California Civil Code § 1709, the California
16 Consumer Privacy Act, and California Penal Code §§ 631-32.

17 128. “Unfair” acts under the UCL have been interpreted using three different tests: (1)
18 whether the public policy which is a predicate to a consumer unfair competition action under the
19 unfair prong of the UCL is tethered to specific constitutional, statutory, or regulatory provisions; (2)
20 whether the gravity of the harm to the consumer caused by the challenged business practice
21 outweighs the utility of the defendant’s conduct; and (3) whether the consumer injury is substantial,
22 not outweighed by any countervailing benefits to consumers or competition, and is an injury that
23 consumers themselves could not reasonably have avoided. Defendants’ conduct is unfair under each
24 of these tests.

25 129. Defendants engaged in business acts or practices deemed “unfair” under the UCL
26 because, as alleged above, Defendants failed to disclose during the Class Period that it was
27 monitoring users while they were not interacting with the Instagram camera feature. *See* Cal. Bus.
28 & Prof. Code § 17200.

1 130. Defendants had a duty to disclose this information because only Defendants had
2 knowledge that they were accessing Plaintiff and Class members' cameras while the Instagram
3 camera feature was not in use.

4 131. This information is material because Plaintiff and Class members would not have
5 downloaded or used the Instagram app if they had known Defendants would secretly monitor and
6 spy on them through their camera.

7 132. In the absence of Defendants' disclosure, Plaintiff and Class members had no way
8 of discovering the material facts about Defendants' access to their smartphone camera prior to the
9 update to iOS.

10 133. Additionally, Defendants' partial representations about when they accessed users'
11 cameras created a duty to disclose the full extent of that interaction. Specifically, Defendants
12 represented to Plaintiff and Class members in their Data Policy that they only access and collect
13 camera data while users are interacting with the Instagram camera feature. This omitted that
14 Defendants also access the user's camera when users are engaging with other parts of the app, such
15 as when a user is scrolling through their feed. Defendant's failure to disclose this information to
16 Plaintiff and Class members concealed the full extent to which they access users' smartphone
17 cameras, including when the camera is not activated by the user.

18 134. Defendants actively concealed that they would access Plaintiff's and Class members'
19 smartphone cameras while the Instagram camera feature was not in use with the intent to induce
20 Plaintiff and Class members to alter their position to their detriment; specifically, to join Instagram
21 and/or remain active users of their social media platform.

22 135. Defendants' conduct violates the policies of the statutes referenced above. Moreover,
23 Defendants' conduct is contrary to public policy, immoral, unethical, oppressive, unscrupulous
24 and/or substantially injurious to consumers. Among other things, it is contrary to the public policy
25 in favor of protecting private information.

26 136. The gravity of the harm of Defendants' secretly monitoring Plaintiff and Class
27 members is significant and there is no corresponding benefit resulting from such conduct. Finally,
28

1 because Plaintiff and Class Members were completely unaware of Defendants' conduct, they could
2 not have possibly avoided the harm.

3 137. Defendants' conduct, as described herein, constitutes a fraudulent business practice
4 within the meaning of the UCL. Defendants have been able to obtain private and confidential
5 information by spying on users through their smartphone camera, all while deceiving Plaintiff and
6 Class members into believing this type of information was private and not monitored or otherwise
7 misused by Defendants.

8 138. Plaintiffs suffered injury as a direct result of Defendants' deceit, including an
9 invasion of their right to privacy. Additionally, Plaintiffs were injured because Defendants obtained
10 their personal and highly confidential information by accessing their smartphone camera without
11 permission. This information is highly valuable and conferred a direct benefit to Defendants, such
12 as boosting their advertisement revenue, to Plaintiffs detriment.

13 139. Plaintiff and Class members have been harmed as a result of Defendants' conduct in
14 violation of the UCL and seek restitution on behalf of themselves and Class members. Additionally,
15 Plaintiff individually and on behalf of the Class, seek an injunction enjoining Defendants from
16 engaging in the unlawful conduct alleged in this claim and requiring Defendants to cease further
17 collection of Plaintiff's and Class members' sensitive personal data, and other appropriate equitable
18 relief, including but not limited to improving its privacy disclosures and obtaining adequately
19 informed consent.

20 **FOURTH CLAIM FOR RELIEF**
21 **Violation of the Wiretap Act, 18 U.S.C. § 2510 *et seq.***
22 **Title 1 of the Electronic Communications Privacy Act ("ECPA")**
23 **(On Behalf of Plaintiff and the Class)**

24 140. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with
25 the same force and effect as if fully restated herein.

26 141. The Federal Wiretap Act, 18 U.S.C. § 2510 *et seq.*, prohibits the interception of any
27 wire, oral, or electronic communications without the consent of at least one authorized party to the
28 communication. The statute confers a civil cause of action on "any person whose wire, oral, or
electronic communication is intercepted, disclosed, or intentionally used in violation of this

1 chapter.” 18 U.S.C. § 2520(a).

2 142. “Oral communication” is defined as “any oral communication uttered by a person
3 exhibiting an expectation that such communication is not subject to interception under
4 circumstances justifying such expectation, but such term does not include any electronic
5 communication[.]” 18 U.S.C. § 2510(2).

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

10 144. “Intercept” is defined as “the aural or other acquisition of the contents of any wire,
11 electronic, or oral communication through the use of any electronic, mechanical, or other device.”
12 18 U.S.C. § 2510(4).

13 145. “Contents” is defined as “includ[ing] any information concerning the substance,
14 purport, or meaning of that communication.” 18 U.S.C. § 2510(8).

15 146. “Person” is defined as “any employee, or agent of the United States or any State or
16 political subdivision thereof, and any individual, partnership, association, joint stock company, trust,
17 or corporation.” 18 U.S.C. § 2510(6).

18 147. Plaintiff and Class members are persons as defined under § 2510(6) of the Act.

19 148. Facebook and Instagram, as corporations, are persons as defined under 18 U.S.C.
20 §2510(6).

21 149. Instagram’s social media application is a device for purposes of the Wiretap Act
22 because it is software used to intercept oral and electronic communication.

23 150. Plaintiff’s and Class members’ private and confidential oral communications that
24 were intercepted in real time by Defendants when Instagram activated their cameras without being
25 prompted by the user, are “oral communications” within the meaning of 18 U.S.C. § 2510(2).

26 151. Plaintiff and Class members reasonably expected that Instagram was not
27 intercepting, recording, or disclosing their oral communications unless Instagram’s camera feature
28

1 was manually activated based on: (i) the context in which these private oral communications
2 occurred, namely Plaintiff's and Class members' homes and other private areas, to which access of
3 all other persons is prohibited absent Plaintiff's and Class members' consent; (ii) a general
4 understanding of how apps, such as, Instagram are supposed to function and based on Instagram's
5 assurances; (iii) Defendants' status as a party who was not an intended party to or recipient of
6 Plaintiff's and Class members' private and confidential communications.

7 152. Pursuant to 18 U.S.C. § 2511(1)(a), Instagram and Facebook, through its design,
8 authorship, programming, knowing and intentional installation, activation, and/or other involvement
9 with the Instagram application, intentionally intercepted, intercepts, or endeavored to intercept, the
10 content of oral communications made by Plaintiff and Class Members without obtaining actual
11 consent from any authorized party to the oral communication.

12 153. Plaintiff's and the Class members' private and confidential oral communications
13 were intercepted during transmission, simultaneous with the communications' arrival, and/or within
14 a second of the communications' arrival without their consent and for the unlawful and/or wrongful
15 purpose of monetizing their private information, including by using their private information to
16 obtain lucrative marketing research, without Plaintiff's and Class members' consent, and for the
17 tortious purpose of committing unfair business practices.

18 154. Interception of Plaintiff's and Class members' private and confidential oral
19 communications without their consent occurs whenever users have the Instagram app open on their
20 smartphone, including when users are not engaging with the Instagram camera feature.

21 155. Plaintiff and Class members could not have, and did not, provide consent to
22 interception of their oral communications because such consent could only apply in instances when
23 users engage with the Instagram camera feature, and not otherwise.

24 156. The practices complained of in this Count fall outside the scope of Defendants'
25 ordinary course of business because they violate Defendants' own policies and public assurances
26 and are in contradiction to the generally understood manner in which social media apps are supposed
27 to function. As such, the surreptitious monitoring of Plaintiff's and Class members' oral
28

1 communications does not facilitate the transmission of the oral communication at issue nor is
2 incidental to such transmission of such communication.

3 157. Defendants’ actions were at all relevant times knowing, willful, and intentional,
4 particularly because Facebook has already come under scrutiny for this same exact conduct less than
5 a year ago. Both times, Defendants conduct has only been disclosed because of updates to Apple’s
6 operating software.

7 158. Defendants intercepted Plaintiff’s and Class members’ oral communications in
8 reckless disregard for Plaintiff’s and Class members’ privacy rights for its own financial benefit,
9 i.e., to obtain lucrative and confidential marketing research it could not otherwise obtain.

10 159. As a result, Plaintiff and Class members have suffered harm and injury due to the
11 interception and transmission of private and personal, confidential, and sensitive communications.

12 160. Pursuant to 18 U.S.C. § 2520, Plaintiff and Class Members have been damaged by
13 the interception, disclosure, and/or use of their communications in violation of the Wiretap Act and
14 are entitled to: (1) appropriate equitable or declaratory relief; (2) damages, in an amount to be
15 determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiff
16 and the Class and any profits made by Google as a result of the violation or (b) statutory damages
17 of whichever is the greater of \$100 per day per violation or \$10,000; and (3) reasonable attorneys’
18 fees and other litigation costs reasonably incurred.

19 **FIFTH CLAIM FOR RELIEF**
20 **Violation of the California Invasion of Privacy Act**
21 **Cal. Penal Code § 631(a)**
22 **(On Behalf of Plaintiff and the Class)**

23 161. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with
24 the same force and effect as if fully restated herein.

25 162. Cal. Penal Code § 630 provides that “[t]he Legislature hereby declares that advances
26 in science and technology have led to the development of new devices and techniques for the
27 purpose of eavesdropping upon private communications and that the invasion of privacy resulting
28

1 from the continual and increasing use of such devices and techniques has created a serious threat to
2 the free exercise of personal liberties and cannot be tolerated in a free and civilized society.”

3 163. Cal. Penal Code § 631(a) prohibits the use of “any machine, instrument, or
4 contrivance, or . . . any other manner” to “intentionally tap[], or make[] unauthorized connection,
5 whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or
6 telephone wire, line, cable, or instrument” *or* to “willfully and without the consent of all parties to
7 the communication, or in any unauthorized manner, read[], or attempt[] to read, or to learn the
8 contents or meaning of any message, report, or communication while the same is in transit or passing
9 over any wire, line, or cable, or is being sent from, or received at any place within this state.”

10 164. Cal. Penal Code § 631(a) further prohibits the “use[], or attempt[] to use, in any
11 manner, or for any purpose, or to communicate in any way, any information so obtained.”

12 165. Pursuant to Cal. Penal Code § 7, Instagram and Facebook, as corporations, are a
13 “person[s].”

14 166. Smartphones constitute a “telegraph or telephone wire, line, cable, or instrument”
15 within the meaning of Cal. Penal Code § 631(a) because they transmit “wire communication”
16 defined in Cal. Penal Code § 629.51 as “any aural transfer made in whole or in part through the use
17 of facilities for the transmission of communications by the aid of wire, cable, or other like connection
18 between the point of origin and the point of reception . . .” *See* Cal. Penal Code § 629.51(a)(1).

19 167. Pursuant to Cal. Penal Code § 629.51(a)(4) “aural transfer means a transfer
20 containing the human voice at any point between and including the point of origin and the point of
21 reception.” *See* Cal. Penal Code § 629.51(a)(4).

22 168. Smartphones constitute “telegraph or telephone wire, line, cable, or instrument”
23 within the meaning of Cal. Penal Code § 631(a) because they transmit “electronic communication”
24 defined in Cal. Penal Code § 629.51(a)(2) as “transfer of signs, signals, writings, images, sounds,
25 data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric,
26 or photooptical system...” *See* Cal. Penal Code § 629.51(a)(2).

27
28

1 169. Defendants Instagram and Facebook acted in a manner to intentionally make an
2 unauthorized connection with Plaintiff and Class members smartphones in direct violation of Cal.
3 Penal Code § 631(a). Specifically, Defendants accessed and monitored users through their
4 smartphone camera without consent and when the Instagram app camera feature was not in use.

5 170. Plaintiff and Class Members reasonably expected, based on a general understanding
6 of how social media applications are supposed to function and Defendants’ own assurances, that
7 Defendants were not accessing, monitoring, or learning the contents of their private communications
8 unless Plaintiff and Class members were interacting with Instagram’s camera feature.

9 171. Defendants were not an intended party or recipient of Plaintiff’s or Class members’
10 confidential communications.

11 172. Plaintiff and Class members could not have provided consent or authorization
12 because such consent or authorization could only apply in situations where they were interacting
13 with Instagram’s camera feature, and not otherwise.

14 173. The private electronic and aural communication that Instagram and Facebook
15 intercepted originated from Plaintiff’s and Class members’ smartphones. The electronic and aural
16 communications that Defendants intercepted were sent to Defendants’ servers, which are, upon
17 information and knowledge, located in the State of California, and were therefore, received “at any
18 place within the state [of California]” within the meaning of Cal. Penal Code § 631(a).

19 174. Defendants’ acts in violation of CIPA occurred in the State of California because
20 those acts resulted from business decisions, practices, and operating policies that Google developed,
21 implemented, and utilized in the State of California.

22 175. Defendants’ acts and practices complained of herein were for the purpose of
23 acquiring and using the content of Plaintiff’s and Class members’ communications to gain lucrative
24 and confidential market research it could not otherwise obtain in violation of Cal. Penal Code § 631.

25 176. Defendants’ actions were at all relevant times knowing, willful, and intentional.
26 Specifically, Defendants have previously admitted to substantially the same conduct with respect to
27 the Facebook application and would have resolved the issue across all Facebook products, including
28

1 Instagram, were this conduct an accident given its egregious nature. Defendants’ actions were done
2 in reckless disregard for Plaintiff’s and Class members’ privacy rights.

3 177. As a result of Defendants’ violations of CIPA, Plaintiff and Class members have
4 suffered harm and injury, including but not limited to the invasion of their privacy rights.

5 178. Defendants are able, and the Court should require them, to implement functionality
6 sufficient to prevent further unauthorized interception of Plaintiff’s and Class members’
7 communications in the future.

8 179. Plaintiff, individually and on behalf of the Class, seeks: (1) an injunction enjoining
9 Plaintiff, individually and on behalf of the Class, seek: (1) an injunction enjoining Defendants from
10 engaging in the unlawful conduct alleged in this claim and requiring Defendants to cease further
11 collection of Plaintiff’s and Class members’ sensitive personal data, and other appropriate equitable
12 relief, including but not limited to improving its privacy disclosures and obtaining adequately
13 informed consent; (2) damages of \$5,000 per violation under Cal. Penal Code § 637.2; and (3) costs
14 and reasonable attorneys’ fees under Cal. Civ. Proc. Code § 1021.5.

15 **SIXTH CLAIM FOR RELIEF**
16 **Violation of the California Invasion of Privacy Act**
17 **Cal. Penal Code § 632**
18 **(On Behalf of Plaintiff and the Class)**

19 180. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with
20 the same force and effect as if fully restated herein.

21 181. Cal. Penal Code § 632 prohibits eavesdropping upon or recording of any confidential
22 communication, including those occurring among the parties in the presence of one another or by
23 means of a telephone, telegraph or other device, through the use of an electronic amplifying or
24 recording device without the consent of all parties to the communication.

25 182. Pursuant to Cal. Penal Code § 7 and § 632(b), Instagram and Facebook, as
26 corporations, are a “person[s].”

27 183. Facebook and Instagram eavesdrop and monitored Plaintiff’s and Class members’
28 confidential communications and activity through their smartphone camera while users were not

1 engaging with Instagram’s camera feature. Facebook and Instagram eavesdropped on users without
2 their consent.

3 184. Plaintiff and Class members could not have provided consent or authorization
4 because such consent or authorization could only apply to instances where they were interacting
5 with Instagram’s camera feature, and not otherwise.

6 185. By spying and monitoring on Plaintiff and Class members without their consent, i.e.,
7 while users were not engaging with Instagram’s camera feature, Defendants “intentionally and
8 without the consent of all parties to a confidential communication” used an “electronic amplifying
9 or recording device” to “eavesdrop upon” Plaintiff and Class members in violation of Cal. Penal
10 Code § 632.

11 186. Defendants’ acts and practices complained of herein were for the purpose of
12 acquiring and using the content of Plaintiff’s and Class members’ communications to gain lucrative
13 and confidential market research it could not otherwise obtain in violation of Cal. Penal Code § 631.

14 187. Defendants’ actions were at all relevant times knowing, willful, and intentional.
15 Specifically, Defendants have previously admitted to substantially the same conduct with respect to
16 the Facebook application and would have resolved the issue across all Facebook products, including
17 Instagram, were this conduct an accident given its egregious nature. Defendants’ actions were done
18 in reckless disregard for Plaintiff’s and Class members’ privacy rights.

19 188. As a result of Defendants’ violations of CIPA, Plaintiff and Class members have
20 suffered harm and injury, including but not limited to the invasion of their privacy rights.

21 189. Defendants are able, and the Court should require them, to implement functionality
22 sufficient to prevent further unauthorized interception of Plaintiff’s and Class members’
23 communications in the future.

24 190. Plaintiff, individually and on behalf of the Class, seek: (1) an injunction enjoining
25 Defendants from engaging in the unlawful conduct alleged in this claim and requiring Defendants
26 to cease further collection of Plaintiff’s and Class members’ sensitive personal data, and other
27 appropriate equitable relief, including but not limited to improving its privacy disclosures and
28

1 obtaining adequately informed consent; (2) damages of \$5,000 per violation under Cal. Penal Code
2 § 637.2; and (3) costs and reasonable attorneys' fees under Cal. Civ. Proc. Code § 1021.5.

3 **SEVENTH CLAIM FOR RELIEF**
4 **Request for Relief Under the Declaratory Judgment Act**
5 **28 U.S.C. § 2201, *et seq.***
6 **(On Behalf of Plaintiff and the Class)**

7 191. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with
8 the same force and effect as if fully restated herein.

9 192. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is
10 authorized to enter a judgment declaring the rights and legal relations of the parties and grant further
11 necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are
12 tortious and that violate the terms of the federal and state statutes described in this complaint.

13 193. An actual controversy has arisen in the wake of Defendants' monitoring users
14 through their smartphone without their consent as alleged herein in violation of Defendants'
15 common law and statutory duties.

16 194. Plaintiff continues to suffer injury and damages as described herein as Defendants
17 continue to monitor Plaintiff's and Class members' through their smartphone camera without their
18 consent.

19 195. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter
20 a judgment declaring, among other things, the following:

- 21
- 22 a. Defendants continued monitoring or otherwise spying on Plaintiff's and Class
23 members constitutes intrusion upon seclusion under the common law.
 - 24 b. Defendants monitoring or otherwise spying on Plaintiff's and Class members is
25 considered "unlawful" conduct pursuant to California Civil Code § 17200, *et seq.*
 - 26 c. Defendants' failure to disclose and/or concealment of the unlawful conduct,
27
- 28

described above, constitutes a violation of California Civil Code § 1709.

d. Defendants’ interception of Plaintiff’s and Class members communications in real-time constitutes a violation of 18 U.S.C. § 2510.

e. Defendants’ unauthorized connection with Plaintiff’s and Class members smartphone devices violated California Penal Code § 631(a).

f. Defendants’ eavesdropping, monitoring, and otherwise spying on Plaintiffs and Class members violated California Penal Code § 632.

g. Defendants’ failure to disclose their data collection practices, including when the Instagram camera feature is not in use, constitutes a violation of the California Consumer Privacy Act.

h. Defendants’ unlawful conduct continues to cause Plaintiff and Class members harm.

196. The Court should also issue corresponding injunctive relief, including but not limited to enjoining Defendants from engaging in the unlawful conduct alleged in this claim and requiring Defendants to cease further monitoring of Plaintiff and Class members, and other appropriate equitable relief, including but not limited to improving its privacy disclosures and obtaining adequately informed consent.

197. If an injunction is not issued, Plaintiff and Class members will suffer irreparable injury and lack an adequate legal remedy in the event of Defendants’ ongoing conduct.

198. Federal and state laws prohibit, among other things, the unlawful monitoring of users without consent. California specifically recognizes privacy as a fundamental right. Given the secretive nature of Defendants’ conduct, the risk of continued violations of federal and California law is real, immediate, and substantial. Plaintiff do not have an adequate remedy at law because many of the resulting injuries are reoccurring and Plaintiff will be forced to bring multiple lawsuits to rectify the same conduct.

1 199. The hardships to Plaintiff and Class members if an injunction is not issued exceeds
2 the hardships to Defendants if an injunction is issued. On the other hand, the cost to Defendants of
3 complying with an injunction by complying with federal and California law and by ceasing to
4 engage in the misconduct alleged herein is relatively minimal, and Defendants have a pre-existing
5 legal obligation to avoid invading the privacy rights of consumers.

6 200. Issuance of the requests injunction will serve the public interest by preventing
7 ongoing monitoring, collection, and misuse of sensitive personal data without consent, thus
8 eliminating the injuries that would result to Plaintiff and the Class, and the potentially hundreds of
9 thousands of consumers who purchased Android Devices.
10

11 **PRAYER FOR RELIEF**

12 WHEREFORE, Plaintiff on behalf of herself and the proposed Class respectfully requests
13 that the Court enter an order:

- 14 A. Certifying the Class and appointing Plaintiff as Class Representative and her counsel
15 as Class Counsel;
- 16 B. Finding that Defendants’ conduct was unlawful as alleged herein;
- 17 C. Awarding such injunctive and other equitable relief as the Court deems just and
18 proper;
- 19 D. Awarding Plaintiff and the Class members statutory, actual, compensatory,
20 consequential, punitive, and nominal damages;
- 21 E. Awarding Plaintiff and the Class members pre-judgment and post-judgment interest;
- 22 F. Awarding Plaintiff and the Class members reasonable attorneys’ fees, costs, and
23 expenses; and
- 24 G. Granting such other relief as the Court deems just and proper.

25 **DEMAND FOR JURY TRIAL**

26 Plaintiff demands a trial by jury for all issues so triable.
27
28

1
2 Dated: September 17, 2020

/s/ Mark N. Todzo
Mark N. Todzo (California Bar No. 168389)
LEXINGTON LAW GROUP
503 Divisadero Street
San Francisco, CA 94117
Telephone: 415-913-7800
Facsimile: 415-759-4112
mtodzo@lexlawgroup.com

7 Christian Levis (*pro hac vice* forthcoming)
8 Amanda Fiorilla (*pro hac vice* forthcoming)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Facsimile: (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com

13 Anthony M. Christina (*pro hac vice* forthcoming)
LOWEY DANNENBERG, P.C.
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA 19428
Telephone: (215) 399-4770
Facsimile: (914) 997-0035
achristina@lowey.com

18 *Attorneys for Plaintiff Brittany Condit and the*
19 *Proposed Class*

CIVIL COVER SHEET

The JS-CAND 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS
Brittany Condit, individually and on behalf of all others similarly situated
(b) County of Residence of First Listed Plaintiff Bergen County, NJ
(c) Attorneys (Firm Name, Address, and Telephone Number)
Mark N. Todzo (California Bar No. 168389), LEXINGTON LAW GROUP
503 Divisadero Street, San Francisco, CA 94117, Telephone: 415-913-7800

DEFENDANTS
Instagram, LLC, and Facebook, Inc.
County of Residence of First Listed Defendant San Mateo, CA
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.
Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)
1 U.S. Government Plaintiff
2 U.S. Government Defendant
3 Federal Question
4 Diversity

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)
Citizen of This State
Citizen of Another State
Citizen or Subject of a Foreign Country
PTF DEF
1 1
2 2
3 3
4 4
5 5
6 6

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Table with columns: CONTRACT, REAL PROPERTY, TORTS, CIVIL RIGHTS, PRISONER PETITIONS, HABEAS CORPUS, OTHER, FORFEITURE/PENALTY, LABOR, IMMIGRATION, BANKRUPTCY, SOCIAL SECURITY, FEDERAL TAX SUITS, OTHER STATUTES.

V. ORIGIN (Place an "X" in One Box Only)
1 Original Proceeding
2 Removed from State Court
3 Remanded from Appellate Court
4 Reinstated or Reopened
5 Transferred from Another District
6 Multidistrict Litigation-Transfer
8 Multidistrict Litigation-Direct File

VI. CAUSE OF ACTION
Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):
Brief description of cause:
Violation of Common Law Invasion of Privacy, Cal. Civ. Code § 1709, California Unfair Competition Law, The Wiretap Act, California Invasion of Privacy Act

VII. REQUESTED IN COMPLAINT: CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, Fed. R. Civ. P. DEMAND \$ JURY DEMAND: Yes No

VIII. RELATED CASE(S), IF ANY (See instructions): JUDGE DOCKET NUMBER

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2) (Place an "X" in One Box Only)
SAN FRANCISCO/OAKLAND SAN JOSE EUREKA-MCKINLEYVILLE

DATE 09/17/2020 SIGNATURE OF ATTORNEY OF RECORD s/Mark N. Todzo