

BURSOR & FISHER, P.A.

L. Timothy Fisher (State Bar No. 191626)
Neal J. Deckant (State Bar No. 322946)
1990 North California Boulevard, Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-Mail: ltfisher@bursor.com
ndeckant@bursor.com

BURSOR & FISHER, P.A.

Scott A. Bursor (State Bar No. 276006)
701 Brickell Avenue, Suite 1420
Miami, FL 33131
Telephone: 305-330-5512
E-Mail: scott@bursor.com

Interim Lead Counsel

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

LAWRENCE OLIN, HAROLD NYANJOM,
SHERON SMITH-JACKSON, JANICE VEGA-
LATKER, BLAKE CARLYLE, MARC
BOEHM, and RAVEN WINHAM individually
and on behalf of all others similarly situated,

Plaintiffs,

v.

FACEBOOK, INC.,

Defendant.

Case No. 3:18-cv-01881-RS

**THIRD AMENDED CONSOLIDATED
CLASS ACTION COMPLAINT**

JURY TRIAL DEMANDED

1 Plaintiffs Lawrence Olin, Harold Nyanjom, Sheron Smith-Jackson, Janice Vega-Latker,
2 Blake Carlyle, Marc Boehm, and Raven Winham (collectively, “Plaintiffs”) bring this action on
3 behalf of themselves and all others similarly situated against Defendant Facebook, Inc.
4 (“Facebook” or “Defendant”). Plaintiffs make the following allegations pursuant to the
5 investigation of their counsel and based upon information and belief, except as to the allegations
6 specifically pertaining to themselves, which are based on personal knowledge.

7 **NATURE OF ACTION**

8 1. Facebook exploited a vulnerability in the permission settings for the Facebook
9 Messenger smartphone application (the “app”) in prior versions of the Android operating system
10 (“OS”). When users install the app, they are prompted to grant Facebook access to the their
11 “contacts” with the following text: “Allow Facebook Messenger access to your contacts?” Below
12 the prompt were choices labeled “Allow” or “Deny.” But upon doing so, the Facebook Messenger
13 app for Android scrape users’ call and text logs. That is, Facebook scrapes *years*’ worth of call and
14 text data, including whether each call was “Incoming,” “Outgoing,” or “Missed,” the date and time
15 of each call, the number dialed, the individual called, and the duration of each call. Facebook then
16 incorporates these data into its profile on each user, which it monetizes for advertising purposes.
17 This vulnerability was later patched in October 2017, at which time Facebook ceased this practice.

18 2. Publicly released emails and messages among Facebook employees show that
19 Facebook knew scraping its users’ call and text logs without permission would be a “pretty high-
20 risk thing to do from a PR perspective,” but that Facebook would nonetheless “charge ahead and
21 do it” (emphasis and highlighting added):
22
23
24
25
26
27
28

From: Mark Tonkelowitz

Sent: Wednesday, February 04, 2015 9:59 PM

To: Joseph Barillari; Mike LeBeau; Mike Vernal; Yul Kwon; Jeremy Galen; Mark Tonkelowitz; Ran Makavy; Evan Ling; Avichal Garg

Subject: Message summary [id.663395043771422]

Michael LeBeau:

>Hey guys, as you all know the growth team is planning on shipping a permissions update on Android at the end of this month. They are going to include the "read call log" permission, which will trigger the Android permissions dialog on update, requiring users to accept the update. They will then provide an in-app opt-in NUX for a feature that lets you continuously upload your SMS and call log history to Facebook to be used for improving things like PYMK, coefficient calculation, feed ranking, etc.

>

>This is a pretty high-risk thing to do from a PR perspective but it appears that the growth team will charge ahead and do it.

>

>Separately, Gravity team had been intending to ship the Bluetooth permission on Android at the same time - in fact we'd already delayed to accommodate more permissions from the growth team, but we didn't realize it was going to be something this risky. We think the risk of PR fallout here is high, and there's some chance that Bluetooth will get pulled into the PR fallout. Screenshot of the scary Android permissions screen becomes a meme (as it has in the past), propagates around the web, it gets press attention, and enterprising journalists dig into what exactly the new update is requesting, then write stories about "Facebook uses new Android update to pry into your private life in ever more terrifying ways - reading your call logs, tracking you in businesses with beacons, etc".

>

>Gravity had a great initial reception. This is because we took painstaking steps to ensure that we had a clear story of user value for the hardware and spoke from a position of transparency but not over-emphasis about the potentially scary bits. But we're still in a precarious position of scaling without freaking people out. If a negative meme were to develop around Facebook Bluetooth beacons, businesses could become reticent to accept them from us, and it could stall the project and its strategy entirely.

>

>So we're still treading very carefully, and of course the growth team is also managing a PR risk of their own with their launch.

3. Despite this, Facebook's emails further demonstrate that it decided to scrape the call logs anyway, and "without subjecting [Facebook users] to an Android permissions dialog at all." (emphasis and highlighting added).

Yul Kwon:

>Also, the Growth team is now exploring a path where we only request Read Call Log permission, and hold off on requesting any other permissions for now.

Yul Kwon:

>Based on their initial testing, it seems that this would allow us to upgrade users without subjecting them to an Android permissions dialog at all.

Yul Kwon:

>It would still be a breaking change, so users would have to click to upgrade, but no permissions dialog screen. They're trying to finish testing by tomorrow to see if the behavior holds true across different versions of Android.

4. The messages show that Facebook was specifically interested in avoiding informing its users that Facebook would be scraping their call and text logs: “Based on their initial testing, it seems that this would allow us to upgrade users without subjecting them to an Android permissions dialog at all. It would still be a breaking change, so users would have to click to upgrade, but no permissions dialog screen.” (emphasis added).

5. Accordingly, Plaintiffs seek compensatory, statutory, and punitive damages, and seek an injunction requiring Facebook to purge its extant call and text logs acquired through these apps.

PARTIES

6. Plaintiff Lawrence Olin is a citizen of New York who resides in New York, New York. Plaintiff Olin installed the Facebook Messenger app on his Android smartphone during the relevant time period, and prior to October 2017, for his personal and household use. Upon initially downloading and installing the Facebook Messenger app, Plaintiff Olin was presented with prompts that read: “Allow Facebook Messenger access to your contacts?” Below the prompts were choices labeled “Allow” or “Deny.” Through this prompt, Plaintiff Olin allowed Facebook Messenger access to his “contacts,” but Plaintiff Olin was never asked whether he consented to Facebook scraping his call and text logs, and never granted Facebook permission to do so. Plaintiff Olin did not consent to Facebook scraping his call and text logs. The Facebook Messenger app scraped his call and text logs, transferred them to Facebook, and monetized these data for advertising purposes. Plaintiff Olin was damaged from the unauthorized theft of his personal, sensitive information because by scraping his call and text logs, Facebook caused him to consume his phone’s resources, including battery, electricity, cellular data, CPU processing power, RAM storage, and hard drive space. Moreover, this information has diminished in value now that Facebook has already stolen and monetized it. The call and text logs Facebook stole are often sold for, and have an established market value of, approximately \$0.05 per individual. Plaintiff Olin did not understand that Facebook Messenger would scrape his call and text logs. Plaintiff Olin would not have installed or used the Facebook Messenger app had he known the truth about the app’s practice of scraping call and text logs. Facebook’s omissions concerning its practice of scraping

1 call and text logs played a substantial part, and so had been a substantial factor, in his decision to
2 install and use Facebook Messenger. Plaintiff Olin attempted to review the call and text logs
3 scraped by Facebook on www.facebook.com, but he was unable to do so because of changes that
4 Facebook made to its website soon after its privacy violation was reported in the press.

5 7. Plaintiff Harold Nyanjom is a citizen of Kansas who resides in Wichita, Kansas.
6 Plaintiff Nyanjom installed the Facebook Messenger app on his Android smartphone during the
7 relevant time period, and prior to October 2017, for his personal and household use. Upon initially
8 downloading and installing the Facebook Messenger app, Plaintiff Nyanjom was presented with
9 prompts that read: “Allow Facebook Messenger access to your contacts?” Below the prompt were
10 choices labeled “Allow” or “Deny.” Through this prompt, Plaintiff Nyanjom allowed Facebook
11 Messenger access to his “contacts,” but Plaintiff Nyanjom was never asked whether he consented
12 to Facebook scraping his call and text logs, and never granted Facebook permission to do so.
13 Plaintiff Nyanjom did not consent to Facebook scraping his call and text logs. The Facebook
14 Messenger app scraped his call and text logs, transferred them to Facebook, and monetized these
15 data for advertising purposes. Plaintiff Nyanjom was damaged from the unauthorized theft of his
16 personal, sensitive information because by scraping his call and text logs, Facebook caused him to
17 consume his phone’s resources, including battery, electricity, cellular data, CPU processing power,
18 RAM storage, and hard drive space. Moreover, this information has diminished in value now that
19 Facebook has already stolen and monetized it. The call and text logs Facebook stole are often sold
20 for, and have an established market value of, approximately \$0.05 per individual. Plaintiff
21 Nyanjom did not understand that Facebook Messenger would scrape his call and text logs.
22 Plaintiff Nyanjom would not have installed or used the Facebook Messenger app had he known the
23 truth about the app’s practice of scraping call and text logs. Facebook’s omissions concerning its
24 practice of scraping call and text logs played a substantial part, and so had been a substantial factor,
25 in his decision to install and use Facebook Messenger. Plaintiff Nyanjom has downloaded and
26 reviewed the call and text logs scraped by Facebook on www.facebook.com. A true and correct
27 redacted excerpt of the data is pictured below:
28

Number:+1316[REDACTED]					
Call Type	Start Time	Duration	Name	Number Label	Number Type
INCOMING	2017-08-21 11:53:11	8			0
Number:+1334[REDACTED]					
Call Type	Start Time	Duration	Name	Number Label	Number Type
OUTGOING	2017-08-09 13:38:43	82			0
MISSED	2017-08-09 13:33:34	0			0
Number:+1316[REDACTED]					
Call Type	Start Time	Duration	Name	Number Label	Number Type
OUTGOING	2017-02-14 11:51:14	0	Momma		1
MISSED	2017-07-03 14:20:55	0	Momma		1
INCOMING	2017-04-09 18:09:45	335	Momma		1
OUTGOING	2017-02-17 11:37:09	4	Momma		1
INCOMING	2017-07-02 14:19:40	70	Momma		1
OUTGOING	2017-04-21 10:39:07	0	Momma		1

8. Plaintiff Sheron Smith-Jackson is a citizen of Texas who resides in Houston, Texas. Plaintiff Smith-Jackson installed the Facebook Messenger app on her Android smartphone during the relevant time period, and prior to October 2017, for her personal and household use. Upon initially downloading and installing the Facebook Messenger app, Plaintiff Smith-Jackson was presented with prompts that read: “Allow Facebook Messenger access to your contacts?” Below the prompt were choices labeled “Allow” or “Deny.” Through this prompt, Plaintiff Smith-Jackson allowed Facebook Messenger access to her “contacts,” but Plaintiff Smith-Jackson was never asked whether she consented to Facebook scraping her call and text logs, and never granted Facebook permission to do so. Plaintiff Smith-Jackson did not consent to Facebook scraping her call and text logs. The Facebook Messenger app scraped her call and text logs, transferred them to Facebook, and monetized these data for advertising purposes. Plaintiff Smith-Jackson was damaged from the unauthorized theft of her personal, sensitive information because by scraping her call and text logs, Facebook caused her to consume her phone’s resources, including battery, electricity, cellular data, CPU processing power, RAM storage, and hard drive space. Moreover,

this information has diminished in value now that Facebook has already stolen and monetized it. The call and text logs Facebook stole are often sold for, and have an established market value of, approximately \$0.05 per individual. Plaintiff Smith-Jackson did not understand that Facebook Messenger would scrape her call and text logs. Plaintiff Smith-Jackson would not have installed or used the Facebook Messenger app had she known the truth about the app's practice of scraping call and text logs. Facebook's omissions concerning its practice of scraping call and text logs played a substantial part, and so had been a substantial factor, in her decision to install and use Facebook Messenger. Plaintiff Smith-Jackson has downloaded and reviewed the call and text logs scraped by the Facebook Messenger app on www.facebook.com. A true and correct redacted excerpt of the data is pictured below:

		Start Time			
		Monday, January 9, 2017 at 3:55pm CST	0		
MISSED	Number+128				
Call Type		Start Time	Duration	Name	Number Label
		Friday, January 6, 2017 at 8:05am CST	19		
OUTGOING	Number+171				
Call Type		Start Time	Duration	Name	Number Label
		Monday, January 9, 2017 at 1:27pm CST	47		
INCOMING					
		Monday, January 9, 2017 at 1:28pm CST	38		
INCOMING	Number+171				
Call Type		Start Time	Duration	Name	Number Label
		Wednesday, January 11, 2017 at 1:34pm CST	1		
OUTGOING					
		Wednesday, January 11, 2017 at 1:33pm CST	510		
OUTGOING					
		Wednesday, January 11, 2017 at 1:32pm CST	54		
OUTGOING					
		Thursday, January 5, 2017 at 2:27pm CST	208		
OUTGOING					

9. Plaintiff Janice Vega-Latker is a citizen of Florida who resides in Boca Raton, Florida. Plaintiff Vega-Latker installed the Facebook Messenger app on her Android smartphone

1 during the relevant time period, and prior to October 2017, for her personal and household use.
2 Upon initially downloading and installing the Facebook Messenger app, Plaintiff Vega-Latker was
3 presented with prompts that read: “Allow Facebook Messenger access to your contacts?” Below
4 the prompt were choices labeled “Allow” or “Deny.” Through this prompt, Plaintiff Vega-Latker
5 allowed Facebook Messenger access to her “contacts,” but Plaintiff Vega-Latker was never asked
6 whether she consented to Facebook scraping her call and text logs, and never granted Facebook
7 permission to do so. Plaintiff Vega-Latker did not consent to Facebook scraping her call and text
8 logs. The Facebook Messenger app scraped her call and text logs, transferred them to Facebook,
9 and monetized these data for advertising purposes. Plaintiff Vega-Latker was damaged from the
10 unauthorized theft of her personal, sensitive information because by scraping her call and text logs,
11 Facebook caused her to consume her phone’s resources, including battery, electricity, cellular data,
12 CPU processing power, RAM storage, and hard drive space. Moreover, this information has
13 diminished in value now that Facebook has already stolen and monetized it. The call and text logs
14 Facebook stole are often sold for, and have an established market value of, approximately \$0.05
15 per individual. Plaintiff Vega-Latker did not understand that Facebook Messenger would scrape
16 her call and text logs. Plaintiff Vega-Latker would not have installed or used the Facebook
17 Messenger app had she known the truth about the app’s practice of scraping call and text logs.
18 Facebook’s omissions concerning its practice of scraping call and text logs played a substantial
19 part, and so had been a substantial factor, in her decision to install and use Facebook Messenger.
20 Plaintiff Vega-Latker has downloaded and reviewed the call and text logs scraped by Facebook on
21 www.facebook.com. A true and correct redacted excerpt of the data is pictured below:
22
23
24
25
26
27
28

		6:44pm EST			
	OUTGOING	Friday, December 25, 2015 at 2:44pm EST	174	Mom	
	OUTGOING	Saturday, December 19, 2015 at 9:49am EST	1674	Mom	
	MISSED	Friday, December 18, 2015 at 5:42pm EST	0	Mom	
	MISSED	Friday, December 18, 2015 at 11:22am EST	0	Mom	
	Number: +1703 [REDACTED]				
	Call Type	Start Time	Duration	Name	Number Label
	MISSED	Monday, March 7, 2016 at 2:02pm EST	0	[REDACTED]	
	OUTGOING	Monday, March 7, 2016 at 2:11pm EST	15	[REDACTED]	
	OUTGOING	Monday, March 7, 2016 at 2:11pm EST	22	[REDACTED]	

10. Plaintiff Blake Carlyle is a citizen of California who resides in Cathedral City, California. Plaintiff Carlyle installed the Facebook Messenger app on his Android smartphone during the relevant time period, in or before 2013, for his personal and household use. Upon initially downloading and installing the Facebook Messenger app, Plaintiff Carlyle was presented with prompts that read: “Allow Facebook Messenger access to your contacts?” Below the prompts were choices labeled “Allow” or “Deny.” Through this prompt, Plaintiff Carlyle allowed Facebook Messenger access to his “contacts,” but Plaintiff Carlyle was never asked whether he consented to Facebook scraping his call and text logs, and never granted Facebook permission to do so. Plaintiff Carlyle did not consent to Facebook scraping his call and text logs. The Facebook Messenger app scraped his call and text logs, transferred them to Facebook in real-time, and monetized these data for advertising purposes. Plaintiff Carlyle was damaged from the unauthorized theft of his personal, sensitive information because by scraping his call and text logs, Facebook caused him to consume his phone’s resources, including battery, electricity, cellular data, CPU processing power, RAM storage, and hard drive space. Moreover, this information has

1 diminished in value now that Facebook has already stolen and monetized it. The call and text logs
2 Facebook stole are often sold for, and have an established market value of, approximately \$0.05
3 per individual. Plaintiff Carlyle did not understand that Facebook Messenger would scrape his call
4 and text logs. Plaintiff Carlyle would not have installed or used the Facebook Messenger app had
5 he known the truth about the app's practice of scraping call and text logs. Facebook's omissions
6 concerning its practice of scraping call and text logs played a substantial part, and so had been a
7 substantial factor, in his decision to install and use Facebook Messenger.

8 11. Plaintiff Marc Boehm is a citizen of California who resides in San Diego,
9 California. Plaintiff Boehm installed the Facebook Messenger app on his Android smartphone
10 during the relevant time period, in or before 2013, for his personal and household use. Upon
11 initially downloading and installing the Facebook Messenger app, Plaintiff Boehm was presented
12 with prompts that read: "Allow Facebook Messenger access to your contacts?" Below the prompts
13 were choices labeled "Allow" or "Deny." Through this prompt, Plaintiff Boehm allowed Facebook
14 Messenger access to his "contacts," but Plaintiff Boehm was never asked whether he consented to
15 Facebook scraping his call and text logs, and never granted Facebook permission to do so. Plaintiff
16 Boehm did not consent to Facebook scraping his call and text logs. The Facebook Messenger app
17 scraped his call and text logs, transferred them to Facebook in real-time, and monetized these data
18 for advertising purposes. Plaintiff Boehm was damaged from the unauthorized theft of his
19 personal, sensitive information because by scraping his call and text logs, Facebook caused him to
20 consume his phone's resources, including battery, electricity, cellular data, CPU processing power,
21 RAM storage, and hard drive space. Moreover, this information has diminished in value now that
22 Facebook has already stolen and monetized it. The call and text logs Facebook stole are often sold
23 for, and have an established market value of, approximately \$0.05 per individual. Plaintiff Boehm
24 did not understand that Facebook Messenger would scrape his call and text logs. Plaintiff Boehm
25 would not have installed or used the Facebook Messenger app had he known the truth about the
26 app's practice of scraping call and text logs. Facebook's omissions concerning its practice of
27 scraping call and text logs played a substantial part, and so had been a substantial factor, in his
28 decision to install and use Facebook Messenger.

12. Plaintiff Raven Winham is a citizen of California who resides in Winchester, California. Plaintiff Winham installed the Facebook Messenger app on her Android smartphone during the relevant time period, in or before 2013, for her personal and household use. Upon initially downloading and installing the Facebook Messenger app, Plaintiff Winham was presented with prompts that read: “Allow Facebook Messenger access to your contacts?” Below the prompts were choices labeled “Allow” or “Deny.” Through this prompt, Plaintiff Winham allowed Facebook Messenger access to her “contacts,” but Plaintiff Winham was never asked whether she consented to Facebook scraping her call and text logs, and never granted Facebook permission to do so. Plaintiff Winham did not consent to Facebook scraping her call and text logs. The Facebook Messenger app scraped her call and text logs, transferred them to Facebook in real-time, and monetized these data for advertising purposes. Plaintiff Winham was damaged from the unauthorized theft of her personal, sensitive information because by scraping his call and text logs, Facebook caused her to consume his phone’s resources, including battery, electricity, cellular data, CPU processing power, RAM storage, and hard drive space. Moreover, this information has diminished in value now that Facebook has already stolen and monetized it. The call and text logs Facebook stole are often sold for, and have an established market value of, approximately \$0.05 per individual. Plaintiff Winham did not understand that Facebook Messenger would scrape her call and text logs. Plaintiff Winham would not have installed or used the Facebook Messenger app had she known the truth about the app’s practice of scraping call and text logs. Facebook’s omissions concerning its practice of scraping call and text logs played a substantial part, and so had been a substantial factor, in her decision to install and use Facebook Messenger.

13. Defendant Facebook, Inc. is a California corporation with its principal place of business located at Menlo Park, California. Facebook is a leading global social media and social networking company. Facebook is a Fortune 500 company with an annual revenue of \$40.653 billion in 2017, and a market capitalization of \$461.75 billion as of March 27, 2018. As part of its operations, Facebook owns and operates the website www.facebook.com, and has developed and distributed smartphone apps for Android and iOS, including the Facebook Messenger app.

14. Whenever reference is made in this Complaint to any representation, act, omission, or transaction of Facebook, that allegation shall mean that Facebook did the act, omission, or transaction through its officers, directors, employees, agents, and/or representatives while they were acting within the actual or ostensible scope of their authority.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of \$5,000,000.00, exclusive of interest and costs, and Plaintiffs, together with most members of the proposed class, are citizens of states different from Facebook.

16. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District. Facebook is a citizen of California, maintains its worldwide corporate headquarters in this District, developed the Facebook Messenger app in this District, distributed and advertised the Facebook Messenger app in this District, formulated its data retention policies in this District, and monetized users' data (including Plaintiffs' data) in this District.

FACTS COMMON TO ALL CAUSES OF ACTION

Background On The Facebook Platform

17. Facebook is the world's leading social networking platform. After registering, users can create a customized profile indicating their name, occupation, interests, schools attended and so on. Users can add other users as "friends," exchange messages, post status updates, read current events in a News Feed, share photos, videos, and links, use various software applications, and receive notifications of other users' activity. Additionally, users may join common-interest user groups organized by workplace, school, hobbies or other topics, and categorize their friends into lists such as "People From Work" or "Close Friends." As of June 2017, Facebook has more than 2 billion active users.

18. Facebook may be accessed by a large range of devices with Internet connectivity, such as desktops, laptops and tablet computers, and smartphones. For example, users can access Facebook by visiting the website www.facebook.com using their web browser on their desktop

1 computer, laptop, phone, or tablet. Alternatively, users can access the Facebook platform by
 2 installing smartphone apps developed by Facebook for Android and iOS, including the Facebook
 3 Messenger app for Android that are at issue in this matter.

4 **Background On Online Advertising And The Value Of User Data To Facebook**

5 19. As used herein, the term “User Data” means a specific profile kept on an Internet
 6 user which is comprised of sets of information that may include an Internet user’s name, country of
 7 origin, browsing habits, areas of interest and hobbies, age, gender, marital status, financial status,
 8 telephone number, email address, buying preferences, and IP address, among other categories.

9 20. In recent years, the online advertising industry has formed into a duopoly between
 10 Facebook and Google, who collectively dominate online advertising. Together, these companies
 11 comprise more than 60% of online advertising sales in the United States. These companies rely
 12 heavily upon so-called “User Data” to target and market advertisements. In a sense, User Data is
 13 the life blood of the online advertising industry.

14 21. As a core component of its business, Facebook collects and compiles User Data.
 15 Facebook does so by offering free services to Internet users, in exchange for the collection of User
 16 Data. Specifically, Facebook operates a leading social media website with over 214 million users
 17 in the United States, and over \$10 billion of annual advertising sales to those users.

18 22. Facebook then monetizes User Data by selling advertising space on its platforms
 19 and services. Advertisers are enticed to place ads with Facebook due to its ability to target specific
 20 demographics and interest groups through each company’s collection of User Data. For all intents
 21 and purposes, Facebook’s dominance over online advertising is maintained and perpetuated by its
 22 treasure trove of User Data.

23 **The Facebook Messenger App for Android Surreptitiously Scrape Users’ Call Logs And Text**
 24 **Data**

25 23. On March 24, 2018, Ars Technica, a leading technology news website, reported that
 26 the Facebook Messenger and Facebook Lite apps for Android are programmed to surreptitiously
 27 scrape users’ call logs and text data without their permission. These data are then sent to Facebook
 28

1 and incorporated into the company's trove of User Data, which in turn are monetized for
2 advertising purposes as discussed above.

3 24. Facebook scrapes users' call logs and text data by exploiting a software
4 vulnerability in the permission settings of older versions of the Android OS. Specifically, when
5 users install the Facebook Messenger app for Android, they are prompted to grant the Facebook
6 Messenger app access to the users' "Contacts" on their Android devices. As explained by a
7 Facebook spokesperson: "The most important part of apps and services that help you make
8 connections is to make it easy to find the people you want to connect with. So, the first time you
9 sign in on your phone to a messaging or social app, it's a widely used practice to begin by
10 uploading your phone contacts." In plain English, Facebook purports to use contact data, in part,
11 as a component of its friend recommendation algorithm.

12 25. However, prior to Android version 4.1, granting Facebook Messenger access to
13 users' "Contacts" also granted Facebook Messenger access to users' call and text logs by default.
14 This vulnerability was patched in later versions of the Android OS, but Android applications
15 (including Facebook Messenger) could bypass this patch by specifying that they were using an
16 older, pre-patched version of the Android Software Development Kit ("SDK"). Ultimately, the
17 Android OS fully deprecated this functionality in all versions of the Android SDK in October 2017.
18 This coincides with the date in which the Facebook Messenger app stopped scraping call and text
19 logs. By comparison, Apple's iOS has never allowed silent access to call and text logs.

20 26. The call logs scraped by Facebook Messenger were discovered by a Facebook user
21 on March 21, 2018. They appear as such:
22
23
24
25
26
27
28

Number: +1 [REDACTED]					
Call Type	Start Time	Duration	Name	Number Label	
OUTGOING	Wednesday, June 1, 2016 at 5:47pm EDT	0	Sean Gallagher		
MISSED	Wednesday, May 25, 2016 at 8:57pm EDT	0	Sean Gallagher		
OUTGOING	Sunday, May 15, 2016 at 1:08pm EDT	0	Sean Gallagher		
INCOMING	Thursday, May 12, 2016 at 5:26pm EDT	10	Sean Gallagher		
OUTGOING	Monday, April 18, 2016 at 3:17pm EDT	10	Sean Gallagher		
OUTGOING	Friday, April 8, 2016 at 6:38pm EDT	27	Sean Gallagher		
MISSED	Wednesday, April 6, 2016 at 2:59pm EDT	0	Sean Gallagher		
OUTGOING	Friday, March 11, 2016 at 4:35pm EST	0	Sean Gallagher		
INCOMING	Tuesday, February 16, 2016 at 9:23am	0	Sean Gallagher		

27. The scraped call logs include whether each call was “Incoming,” “Outgoing,” or “Missed.” They also include the date and time of each call, the number dialed, the individual called, and the duration of each call. These call logs may contain *years* worth of call data. The scraped text logs contain similar data.

28. On March 25, 2018, a Facebook spokesperson admitted that Facebook collects such data. Yet, as Ars Technica reported, “Facebook never explicitly revealed that the data was being collected,” and that “there was never an explicit message requesting access to phone call and SMS [text] data.”

29. On June 5, 2018, the New York Times reported that Facebook has a data sharing agreement with Huawei, a Chinese telecommunications company. American citizens have recently been warned by the FBI, CIA, and NSA to not use Huawei’s products or services, as it would give Huawei “the capacity to maliciously modify or steal information” and provide Huawei “the capacity to conduct undetected espionage.” Facebook officials said in an interview that the company would wind down the Huawei deal by June 2018.

1 30. On June 29, 2018, Facebook produced 747 pages of documents to Congress, which
2 show that Facebook has agreements in place to share its user data with 61 different entities. These
3 entities include Apple, UPS, Microsoft, Blackberry, and Samsung. Accordingly, Facebook shares
4 or disseminates the scraped user data with these 61 entities.

5 31. Recently, the Open Handset Alliance, the working group responsible for developing
6 the Android OS, announced that it plans to change the permission settings in the next version of
7 Android. These changes to the permission serve to prevent or curtail the exact data scraping
8 practices at issue here. Specifically, the Open Handset Alliance created a new permission group
9 specifically concerning call and text log data. Under these new permissions, users will need to
10 specifically “opt-in” to the sharing of their call and text logs.

11 32. Member of Parliament Damian Collins, chair of the Digital, Culture, Media and
12 Sport Committee, recently investigated Facebook’s conduct in connection with a lawsuit brought
13 by a third-party app developer, Six4Three. Upon completion of the Committee’s investigation, Mr.
14 Collins’ findings were summarized in relevant part as follows: “Facebook knew that the changes
15 to its policies on the Android mobile system, which enabled the Facebook app to collect a record of
16 calls and texts sent by the user would be controversial. To mitigate any bad PR, Facebook planned
17 to make it as hard of possible for users to know that this was one of the underlying features of the
18 upgrade of their app.” A screenshot of this summary is pictured below:

Note by Damian Collins MP, Chair of the DCMS Committee**Summary of key issues from the Six4Three files****1. White Lists**

Facebook have clearly entered into whitelisting agreements with certain companies, which meant that after the platform changes in 2014/15 they maintained full access to friends data. It is not clear that there was any user consent for this, nor how Facebook decided which companies should be whitelisted or not.

2. Value of friends data

It is clear that increasing revenues from major app developers was one of the key drivers behind the Platform 3.0 changes at Facebook. The idea of linking access to friends data to the financial value of the developers relationship with Facebook is a recurring feature of the documents.

3. Reciprocity

Data reciprocity between Facebook and app developers was a central feature in the discussions about the launch of Platform 3.0.

4. Android

Facebook knew that the changes to its policies on the Android mobile phone system, which enabled the Facebook app to collect a record of calls and texts sent by the user would be controversial. To mitigate any bad PR, Facebook planned to make it as hard of possible for users to know that this was one of the underlying features of the upgrade of their app.

CLASS REPRESENTATION ALLEGATIONS

33. Plaintiffs seek to represent a class defined as all persons in the United States who installed the Facebook Messenger app for Android, and granted Facebook permission to access their “Contacts” (the “Class” or “Nationwide Class”).

34. Plaintiffs Carlyle, Boehm, and Winham also seek to represent a subclass defined as all members of the Class Members in the State of California (the “Subclass” or “California Subclass”).

35. Members of the Class and Subclass are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Class and Subclass number in the millions. The precise number of Class and Subclass members and their identities are unknown to Plaintiffs at this time but may be determined through discovery. Class and Subclass members

1 may be notified of the pendency of this action by mail and/or publication through the distribution
2 records of Defendant and third-party retailers and vendors.

3 36. Common questions of law and fact exist as to all Class and Subclass members and
4 predominate over questions affecting only individual Class and Subclass members. Common legal
5 and factual questions include, but are not limited to: whether Facebook scraped call and text logs
6 through the Facebook Messenger app for Android; whether Facebook scraped these data by
7 exploiting a vulnerability in the Android permission settings; and whether Defendant committed
8 statutory and common law fraud by doing so.

9 37. The claims of the named Plaintiffs are typical of the claims of the Class and
10 Subclass in that the named Plaintiffs installed the Facebook Messenger app for Android prior to
11 October 2017 and granted permission for Facebook to access their “Contacts,” but did not consent
12 to the scraping of their call and text logs.

13 38. Plaintiffs are adequate representatives of the Class and Subclass because their
14 interests do not conflict with the interests of the Class and Subclass members they seek to
15 represent, they have retained competent counsel experienced in prosecuting class actions, and they
16 intend to prosecute this action vigorously. The interests of Class and Subclass members will be
17 fairly and adequately protected by Plaintiffs and their counsel.

18 39. The class mechanism is superior to other available means for the fair and efficient
19 adjudication of the claims of the Class. Each individual Class member may lack the resources to
20 undergo the burden and expense of individual prosecution of the complex and extensive litigation
21 necessary to establish Defendant’s liability. Individualized litigation increases the delay and
22 expense to all parties and multiplies the burden on the judicial system presented by the complex
23 legal and factual issues of this case. Individualized litigation also presents a potential for
24 inconsistent or contradictory judgments. In contrast, the class action device presents far fewer
25 management difficulties and provides the benefits of single adjudication, economy of scale, and
26 comprehensive supervision by a single court on the issue of Defendant’s liability. Class treatment
27 of the liability issues will ensure that all claims and claimants are before this Court for consistent
28 adjudication of the liability issues.

COUNT I
**Violation Of California's Computer Data Access and
Fraud Act, Cal. Pen. Code, § 502**

40. Plaintiffs incorporate by reference and re-allege herein all paragraphs alleged above.

41. Plaintiffs bring this claim individually and on behalf of the members of the
Nationwide Class.

42. Defendant knowingly accessed and without permission used Plaintiffs' and Class
members' data in order to wrongfully control or obtain property or data in violation of California
Penal Code § 502(c)(1).

43. Defendant knowingly accessed and without permission took, copied, and/or used
data from Plaintiffs' and Class members' computers, computer systems and/or computer network
in violation of California Penal Code § 502(c)(2).

44. Defendant knowingly and without permission used or caused to be used Plaintiffs'
and Class members' computer services in violation of California Penal Code § 502(c)(3).

45. Defendant knowingly and without permission accessed or caused to be accessed
Plaintiffs' and Class members' computers, computer systems, and/or computer network in
violation of California Penal Code § 502(c)(7).

46. Plaintiffs and Class members suffered and continue to suffer damage as a result of
Defendant's violations of the California Penal Code § 502 identified above. Plaintiffs have also
suffered damage from the unauthorized theft of their personal, sensitive information because by
scraping the call and text logs, Facebook caused Plaintiffs to use up their phones' resources,
including battery, electricity, cellular data, CPU processing power, RAM storage, and hard drive
space. Moreover, this information has diminished in value now that Facebook has already stolen
and monetized it. The call and text logs Facebook stole are often sold for, and have an established
market value of, \$0.05 per individual. Defendant's conduct also caused irreparable and
incalculable harm and injuries to Plaintiffs and Class members in the form of invading their
privacy, and, unless enjoined, will cause further irreparable and incalculable injury, for which
Plaintiffs and Class members have no adequate remedy at law.

47. Defendant willfully violated California Penal Code § 502 in disregard and derogation of the rights of Plaintiffs and Class members, and Defendant's actions as alleged above were carried out with oppression, fraud and malice.

48. Pursuant to California Penal Code § 502(e), Plaintiffs and Class members are entitled to injunctive relief, compensatory damages, punitive or exemplary damages, attorneys' fees, costs and other equitable relief.

COUNT II

California Constitutional Right to Privacy

49. Plaintiffs incorporate by reference and re-allege herein all paragraphs alleged above.

50. Plaintiffs bring this claim individually and on behalf of the members of the Nationwide Class.

51. Plaintiffs and Class members have a legally protected privacy interest in their call logs and text data, as codified, among other places, in California's Computer Data Access and Fraud Act, Cal. Pen. Code, § 502.

52. Plaintiffs and Class members had a reasonable expectation of privacy in their data given that Defendant did not disclose that it was collecting Plaintiffs' and Class members' call logs and text data and such data is necessarily of a highly sensitive and private nature.

53. Defendant's conduct in surreptitiously collecting this data constituted a serious violation of Plaintiffs' and Class members' privacy interests.

COUNT III

Intrusion Upon Seclusion

54. Plaintiffs incorporate by reference and re-allege herein all paragraphs alleged above.

55. Plaintiffs bring this claim individually and on behalf of the members of the Nationwide Class.

56. Plaintiffs and Class members had a reasonable expectation of privacy in their call logs and text data – data that they did not give Defendant permission to access.

57. Defendant intentionally intruded into Plaintiffs' and Class members' private information by collecting their call logs and text data without their permission and without providing notice.

58. This intrusion into Plaintiffs' and Class members' private information would be highly offensive to a reasonable person.

59. Defendant's intrusion of seclusion caused damage to Plaintiffs and Class members by invading their privacy and depriving them of any income that Defendant generated through its unauthorized use or sale of their call logs and text data.

COUNT IV **Unjust Enrichment**

60. Plaintiffs incorporate by reference and re-allege herein all paragraphs alleged above.

61. Plaintiffs bring this claim individually and on behalf of the members of the Nationwide Class.

62. Plaintiff and Class members conferred a benefit upon Defendant by providing it, unwittingly, with call logs and text data. Defendant profited from this collection of data by incorporating it into its profile on each user, which it monetized for advertising purposes.

63. Because Defendant's retention of the non-gratuitous benefits conferred on it by Plaintiffs and Class members is unjust and inequitable, Defendant must pay restitution to Plaintiffs and Class members for its unjust enrichment, as ordered by the Court.

COUNT V **Fraud**

64. Plaintiffs hereby incorporate by reference the allegations contained in all preceding paragraphs of this complaint.

65. Plaintiffs bring this claim individually and on behalf of the members of the Nationwide Class.

66. As discussed above, Defendant failed to disclose to class members that by installing and downloading the Facebook Messenger app, Facebook would steal Plaintiffs' and class members' call and text logs without permission.

67. The false and misleading representations and omissions were made with knowledge of their falsehood.

68. The false and misleading representations and omissions were made by Defendant, upon which Plaintiffs and members of the Nationwide Class reasonably and justifiably relied, and

were intended to induce and actually induced Plaintiffs and Class members to use the Facebook Messenger app.

69. The fraudulent actions of defendant caused damage to Plaintiffs and members of the Nationwide Class, who are entitled to damages and other legal and equitable relief as a result.

COUNT VI
Violation Of The California Invasion Of Privacy Act,
Cal. Penal Code § 631

70. Plaintiffs hereby incorporate by reference the allegations contained in all preceding paragraphs of this complaint.

71. Plaintiffs Carlyle, Boehm, and Winham bring this claim individually and on behalf of the members of the proposed Subclass against Defendant.

72. To establish liability under section 631(a), Plaintiffs need only establish that Defendants, “by means of any machine, instrument, contrivance, or in any other manner,” did any of the following:

Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,

Or

Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state,

Or

Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,

Or

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.

73. Section 631(a) is not limited to phone lines, but also applies to “new technologies” such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21

(N.D. Cal. Aug. 12, 2016) (CIPA applies to “new technologies” and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134, at *5-6 (N.D. Cal. Dec. 22, 2006) (CIPA governs “electronic communications”); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook’s collection of consumers’ Internet browsing history).

74. Defendant’s Facebook Messenger application, including the software used to employ data scraping, is a “machine, instrument, contrivance, or ... other manner” used to engage in the prohibited conduct at issue here.

75. At all relevant times, by deploying Facebook Messenger, Defendant intentionally tapped, electrically or otherwise, the lines of internet communication between Plaintiffs and Subclass Members on the one hand, and Facebook Messenger on the other hand.

76. At all relevant times, by deploying Facebook Messenger, Defendant willfully and without the consent of all parties to the communication, or in any unauthorized manner, read or attempted to read or learn the contents or meaning of electronic communications of Plaintiffs and putative Subclass Members, while the electronic communications were in transit or passing over any wire, line or cable or were being sent from or received at any place within California.

77. Defendant implemented Facebook Messenger’s software to accomplish the wrongful conduct at issue here.

78. Plaintiffs and Subclass Members did not consent to any of Defendant’s actions in implementing Facebook Messenger’s data scrape software/functionality. Nor have Plaintiffs nor Class Members consented to Defendant’s intentional access, interception, reading, learning, recording, and collection of Plaintiffs’ and Class Members’ electronic communications.

79. The violation of section 631(a) constitutes an invasion of privacy sufficient to confer Article III standing.

80. Plaintiffs and Class Members seek all relief available under Cal. Penal Code § 637.2, including statutory damages of \$5,000 per violation.

COUNT VII
Violation Of The California Invasion Of Privacy Act,
Cal. Penal Code § 632

81. Plaintiffs hereby incorporate by reference the allegations contained in all preceding paragraphs of this complaint.

82. Plaintiffs Carlyle, Boehm, and Winham bring this claim individually and on behalf of the members of the proposed Subclass against Defendant.

83. California Penal Code § 632(a) provides, in pertinent part:

A person who, intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio, shall be punished by a fine not exceeding two thousand five hundred dollars

84. Defendant is a “person” under the California Invasion of Privacy Act.

85. At all relevant times, by scraping Plaintiffs’ call and text metadata without permission, Defendant intentionally used an electronic amplifying or recording device to eavesdrop upon and record the confidential communications of Plaintiffs and Subclass Members.

86. When using Facebook Messenger, Plaintiffs and Subclass Members had an objectively reasonable expectation of privacy. Plaintiffs and Subclass Members did not reasonably expect that Defendant would intentionally use an electronic amplifying or recording device to eavesdrop upon and record the confidential communications of Plaintiffs and Subclass Members.

87. Plaintiffs and Subclass Members did not consent to any of Defendant’s actions in scraping their call and text metadata while using the Facebook Messenger app. Nor have Plaintiffs or Subclass Members consented to Defendant’s intentional use of an electronic amplifying or recording device to eavesdrop upon and record the confidential communications of Plaintiffs and Subclass Members.

88. Plaintiffs and Subclass Members have suffered loss by reason of these violations, including, but not limited to, violation of the right of privacy and loss of value in their PII.

89. Pursuant to Cal. Penal Code § 637.2, Plaintiffs and Subclass Members have been injured by the violations of Cal. Penal Code § 632, and each seek damages for the greater of \$5,000 or three times the amount of actual damages, as well as injunctive relief.

COUNT VIII
Violation Of The California Invasion Of Privacy Act,
Cal. Penal Code § 635

90. Plaintiffs hereby incorporate by reference the allegations contained in all preceding paragraphs of this complaint.

91. Plaintiffs Carlyle, Boehm, and Winham bring this claim individually and on behalf of the members of the proposed Subclass against Defendant.

92. California Penal Code § 635 provides, in pertinent part:

Every person who manufactures, assembles, sells, offers for sale, advertises for sale, possesses, transports, imports, or furnishes to another any device which is primarily or exclusively designed or intended for eavesdropping upon the communication of another, or any device which is primarily or exclusively designed or intended for the unauthorized interception or reception of communications between cellular radio telephones or between a cellular radio telephone and a landline telephone in violation of Section 632.5, or communications between cordless telephones or between a cordless telephone and a landline telephone in violation of Section 632.6 , shall be punished by a fine not exceeding two thousand five hundred dollars.

93. At all relevant times, by deploying Facebook Messenger's data scrape software/functionality, each Defendant intentionally manufactured, assembled, sold, offered for sale, advertised for sale, possessed, transported, imported, and/or furnished a wiretap device that is primarily or exclusively designed or intended for eavesdropping upon the communication of another.

94. Facebook Messenger's data scrape software/functionality is a "device" that is "primarily or exclusively designed" for eavesdropping. That is, Facebook Messenger's data scrape software/functionality was designed to gather PII, including call and text metadata, and other electronic communications.

95. Plaintiffs and Subclass Members did not consent to any of Defendant's actions in implementing Facebook Messenger's data scrape.

96. Plaintiffs and Subclass Members seek all relief available under Cal. Penal Code § 637.2, including statutory damages of \$5,000 per violation.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seek judgment against Defendant, as follows:

- a. For an order certifying the Nationwide Class and Subclass under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiffs as the representatives of the Class and Subclass and Plaintiffs' attorneys as Class Counsel to represent members of the Class and Subclass;
- b. For an order declaring the Defendant's conduct violates the statutes referenced herein;
- c. For an order finding in favor of Plaintiffs and the Nationwide Class and Subclass on all counts asserted herein;
- d. For compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury;
- e. For prejudgment interest on all amounts awarded;
- f. For an order of restitution and all other forms of equitable monetary relief; and
- g. For an order awarding Plaintiffs, the Nationwide Class, and Subclass their reasonable attorneys' fees and expenses and costs of suit.

DEMAND FOR TRIAL BY JURY

Plaintiffs demand a trial by jury of all issues so triable.

Dated: December 18, 2020

Respectfully submitted,

BURSOR & FISHER, P.A.

By: /s/ L. Timothy Fisher
L. Timothy Fisher

L. Timothy Fisher (State Bar No. 191626)
Neal J. Deckant (State Bar No. 322946)
1990 North California Boulevard, Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455

Facsimile: (925) 407-2700
E-Mail: ltfisher@bursor.com
ndeckant@bursor.com

BURSOR & FISHER, P.A.
Scott A. Bursor (State Bar No. 276006)
701 Brickell Avenue, Suite 1420
Miami, FL 33131
Telephone: 305-330-5512
E-Mail: scott@bursor.com

Interim Lead Counsel