

1 Brian J. Dunne (CA 275689)  
bdunne@bathaedunne.com  
2 **BATHAEE DUNNE LLP**  
633 West Fifth Street, 26th Floor  
3 Los Angeles, CA 90071  
4 Tel: (213) 462-2772

5 Yavar Bathaee (CA 282388)  
yavar@bathaedunne.com  
6 Edward M. Grauman\* (NY 4196390)  
egrauman@bathaedunne.com  
7 Andrew C. Wolinsky\* (NY 4892196)  
awolinsky@bathaedunne.com  
8 **BATHAEE DUNNE LLP**  
9 445 Park Avenue, 9th Floor  
New York, NY 10022  
10 Tel: (332) 205-7668

11 *Attorneys for Plaintiffs*

12  
13  
14 **UNITED STATES DISTRICT COURT**  
15 **NORTHERN DISTRICT OF CALIFORNIA**  
16

17 Adam Bauer, on behalf of himself and )  
all others similarly situated, )

18 )  
19 *Plaintiffs,* )

20 vs. )

21 LinkedIn Corporation, )

22 *Defendant.* )  
23 )  
24 )  
25 )  
26 )

Case Number: \_\_\_\_\_

**Class Action Complaint**  
Jury Trial Demanded

27  
28  
\* *Pro hac vice* to be sought.

**TABLE OF CONTENTS**

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

PAGE

PARTIES ..... 3

I. DEFENDANT..... 3

II. PLAINTIFF ..... 3

JURISDICTION AND VENUE ..... 4

FACTS ..... 5

I. THE APPLE UNIVERSAL CLIPBOARD ..... 5

    A. Apple’s Handoff Feature..... 5

    B. The Universal Clipboard ..... 6

II. UNIVERSAL CLIPBOARD, ELECTRONIC COMMUNICATIONS, AND THE UNDERSTANDING AND EXPECTATION OF PRIVACY ..... 9

III. LINKEDIN’S IOS APP REPEATEDLY READS THE CONTENTS OF THE UNIVERSAL CLIPBOARD WITHOUT USER PERMISSION ..... 12

CLASS ACTION ALLEGATIONS ..... 17

CLAIMS FOR RELIEF ..... 20

PRAYER FOR RELIEF ..... 40

JURY DEMAND ..... 41

INTRODUCTION

1  
2 1. This lawsuit seeks to remedy a particularly brazen, indefensible privacy violation  
3 perpetrated *en masse* by one of the world’s largest and most trusted social networks, LinkedIn.  
4 Until abruptly exposed by Apple and independent developers, LinkedIn had programmed its  
5 iPhone and iPad applications to abuse Apple’s Universal Clipboard to brazenly read and divert  
6 LinkedIn users’ most sensitive data—including sensitive data *from other Apple devices*—without  
7 their consent or knowledge. LinkedIn’s conduct violated federal and State law, and harmed  
8 hundreds of thousands—if not millions—of LinkedIn users, including Plaintiff. Plaintiff brings  
9 this action on behalf of himself and others similarly situated.

10 \* \* \*

11 2. In Apple’s most recent beta release of its iOS mobile device operating system—  
12 iOS 14—Apple added a new privacy setting that allows users to receive a notification each time  
13 an app on their iPhone or iPad reads from the system clipboard. Many commenters hailed this and  
14 related new features in iOS 14 as an important step toward improved data privacy in mobile devices  
15 and their applications.

16 3. But when developers and other beta testers began using the new privacy  
17 notifications in iOS 14, they discovered something quite disturbing: LinkedIn’s mobile application  
18 for iPhones and iPads was secretly reading users’ clipboards. A lot. Constantly, even.

19 4. Specifically, as of July 2, 2020, LinkedIn’s iOS App was, after each user keystroke,  
20 immediately reading the contents of the device’s system clipboard—the temporary storage where  
21 users “cut” or “copy” information to for their *own* later use through a “paste” command in a  
22 particular app and location.

23 5. The system clipboard often contains some of the most sensitive data users routinely  
24 and temporarily store on their devices. Indeed, users store information, such as photos, text  
25 messages, e-mails, cryptographic keys, or even medical records, in their device clipboards to name  
26 a few examples. And LinkedIn was surreptitiously reading it—again and again and again—without  
27 any user-triggered paste commands, and without even notifying the user.  
28

1           6.       LinkedIn’s conduct, which continued for potentially years before Apple’s iOS 14  
2 beta laid bare its existence, was particularly egregious for users with more than one Apple device.

3           7.       A feature on Apple iOS and MacOS devices called the Universal Clipboard allows  
4 nearby devices to share clipboard information. Thus, a photo “copied” on a Mac computer is  
5 instantly transferred to a nearby iPhone’s clipboard—but it only remains available to a user on that  
6 device for 120 seconds for security reasons.

7           8.       Yet the LinkedIn App doesn’t just cut the user out of the clipboard equation—it  
8 circumvents the 120 second timeout on Apple’s Universal Clipboard. Specifically, the LinkedIn  
9 App repeatedly reads the Universal Clipboard with every user keystroke, and these “reads” are  
10 interpreted by Apple’s Universal Clipboard as a “paste” command, which takes the temporary  
11 information in the Universal Clipboard and removes the 120 second timeout. Simply put, LinkedIn  
12 has not only been spying on its users, it has been spying *on their nearby computers and other*  
13 *devices*, and it has been *circumventing* Apple’s Universal Clipboard timeout policy in doing so.

14           9.       Users expect the information that they place in their clipboard, including their  
15 Universal Clipboard, to remain available only to them, to be used only with their consent. Indeed,  
16 information such as photos, text and e-mail messages, voice recordings, and other  
17 communications, are expected to remain in a clipboard until the user herself issues a paste  
18 command or overwrites the information. LinkedIn ignored that expectation and intentionally and  
19 repeatedly invaded user privacy—and it carefully hid what it was doing from users, knowing just  
20 how far beyond the boundaries of reasonable conduct it had gone.

21           10.      The LinkedIn App’s egregious behavior was never disclosed to users. Indeed, until  
22 recently, users had no idea that their most sensitive communications were being indiscriminately  
23 intercepted and read by the LinkedIn App, including prior to, or contemporaneously with,  
24 transmission from one device to another.

25           11.      This action seeks to hold LinkedIn responsible for its misbehavior.  
26  
27  
28

**PARTIES**

**I. DEFENDANT**

12. Defendant LinkedIn is a Sunnyvale, California-based corporation incorporated under the laws of Delaware.

13. LinkedIn is a social network focusing on professional connections. It has approximately 675 million members worldwide, including within its membership executives from every Fortune 500 company.

14. LinkedIn itself has over 10,000 employees and offices worldwide, with its headquarters at 10000 W. Maude, Sunnyvale, CA 94085.

15. On Apple computer desktops, users typically interact with LinkedIn using a web browser, but on mobile devices, such as iPhones and iPads, users predominantly use LinkedIn’s native mobile app for iOS (the “LinkedIn App”).

**II. PLAINTIFF**

16. Plaintiff Adam Bauer (“Plaintiff”) is a natural person who resides in New York, New York. Plaintiff routinely uses the LinkedIn App on his iPhone and iPad devices. Plaintiff has a valid and active LinkedIn account, which he uses (and during the Class Period used) in conjunction with the LinkedIn App to interact with the LinkedIn social network.

17. Plaintiff routinely and frequently uses (and during the Class Period used) the LinkedIn App within proximity of his other Apple devices, including Macintosh computers. All of his devices, including his Macintosh computers are logged in using, and associated with, the same iCloud account.

18. Plaintiff has (and during the Class Period had) Handoff and Universal Clipboard enabled on his devices.

19. Plaintiff routinely stores (and during the Class Period stored) sensitive information in his device clipboards on a temporary basis, including, for example, pictures, videos, audio recordings, and portions of e-mails and text messages.



1 **FACTS**

2 **III. THE APPLE UNIVERSAL CLIPBOARD**

3 **A. Apple’s Handoff Feature**

4 27. In the summer of 2014, Apple announced a new set of features on its iOS and  
5 MacOS devices that allowed information to move seamlessly among certain of those devices. For  
6 example, a user viewing a web page on their desktop could, for the first time, resume viewing the  
7 same webpage on a mobile device, such as an iPhone. Apple calls this functionality Handoff.

8 28. Handoff is enabled on MacOS and iOS devices by default and remains active for  
9 most applications unless expressly turned off by a user.

10 29. Handoff implements what Apple calls continuity features. As Apple describes on  
11 its support site, Handoff allows a user to pick up where they left off:

12 **Pick up where you left off with Handoff on Mac**

13 With Handoff, you can start something on one device (Mac, iPhone,  
14 iPad, or Apple Watch) and then pick it up on another without losing  
15 focus on what you’re doing. For example, look at a webpage on your  
16 iPhone, then pick up where you left off in Safari on your Mac. You  
17 can use Handoff with many Apple apps—for example, Calendar,  
18 Contacts, Pages, or Safari. Some third-party apps may also work  
19 with Handoff.

20 30. To accomplish Handoff functionalities, Apple relies on several components,  
21 including Apple’s iCloud system, Bluetooth Low Energy (“BLE”) and wireless networking (*e.g.*,  
22 WiFi, LTE) subsystems on each Apple device, and the contents of temporary storage stored in  
23 each device’s random-access memory (“RAM”).

24 31. These components work together to allow the seamless discovery of an iCloud  
25 user’s nearby Apple devices and transmission of information across those devices, including  
26 iPhones, iPads, and Macintosh desktop computers.

27 32. Handoff requires that Apple’s “continuity” conditions be met, which include that:  
28 (a) a source device (*e.g.*, iPhone, iPad, Mac) is signed into Apple’s iCloud with an authenticated  
Apple ID and has BLE and wireless networking components enabled; and (b) each potential  
continuity device (*i.e.*, a different iPhone, iPad, or Mac) is within BLE range and is authenticated

1 with Apple’s iCloud system using the same Apple ID. If any continuity conditions are not met on  
2 a particular continuity-capable device (*e.g.*, iPhone, iPad, or Mac running iOS 10+/Mac OS  
3 10.10+), Handoff is not allowed to transmit information across devices.

4 33. Handoff-enabled applications on Apple devices generally send information used in  
5 common applications—for example, Apple’s Safari web browser, Apple’s Messages app, and  
6 Apple’s News and Books e-reading apps.

7 34. Handoff-enabled applications initiate various messages intended for nearby  
8 continuity-capable devices as the user uses an application; these messages are exchanged between  
9 and among devices when Handoff-enabled applications are opened or closed or upon some user-  
10 triggered event.

11 **B. The Universal Clipboard**

12 35. In 2016, Apple extended Handoff to a well-known operating system feature—the  
13 system clipboard. Indeed, clipboard functionality has been part of every major operating system  
14 for several decades. A clipboard has traditionally been a temporary place to store text or other  
15 content, such that the information stored on the clipboard can be placed in another location or in  
16 another application.

17 36. Information is “cut” or “copied” to a clipboard, and then “pasted” in another  
18 location. If information is “cut” from a location, it is removed from that location and placed in the  
19 clipboard. If it is copied, it remains in the original location and a copy is placed on the clipboard.  
20 Information on the clipboard remains there until the user expresses an intent to place the  
21 information in a particular location.

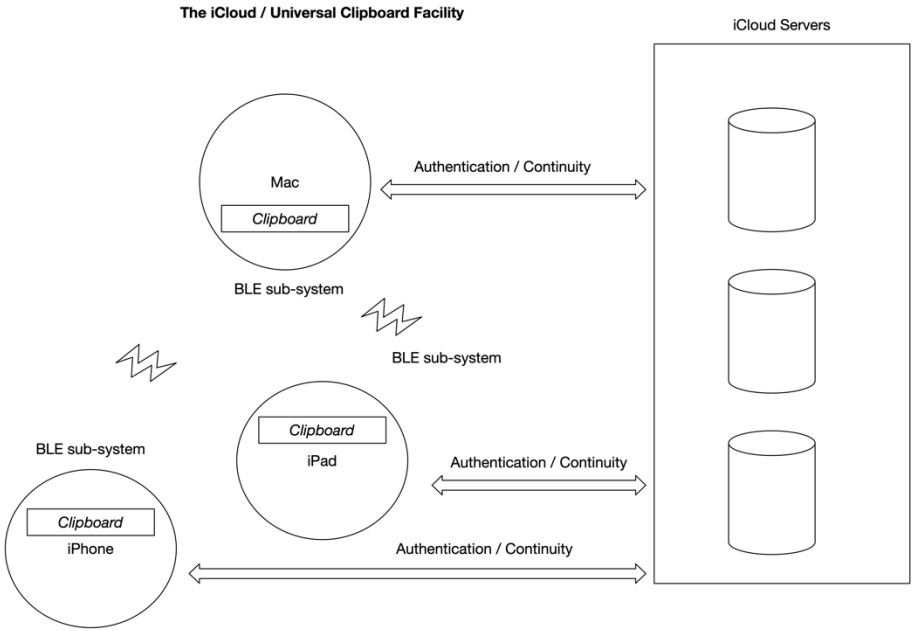
22 37. Without a paste action, a user’s copied or cut data remains in the clipboard until  
23 another copy or cut command overwrites that information. Generally, clipboards store only one  
24 thing at a time, though some specialized clipboards, such as those in certain applications, have  
25 “histories” that allow several things to be copied to a clipboard. Apple’s system clipboard does not  
26 implement a “history” feature. It stores only one thing at a time.



1 38. Clipboards are typically memory locations on a local computer and are not  
2 transmitted across devices or to a centralized server. They remain in temporary storage—in most  
3 instances in memory allocated by the operating system in a device’s RAM.

4 39. As part of the new Handoff functionality, Apple in 2016 announced a Universal  
5 Clipboard that allowed information copied or cut to a clipboard on one device to be accessible on  
6 another. Thus, for example, a user could copy the contents of a text message on his iPhone and  
7 paste it into an application open on his iPad.

8 40. The Universal Clipboard is a facility that (a) discovers nearby devices,  
9 (b) interfaces with Apple’s cloud-based servers, iCloud, for authentication and other coordination,  
10 (c) initiates the transmission of information using each device’s BLE and other wireless  
11 networking subsystems, and (d) ensures that information in the Universal Clipboard expires after  
12 a two-minute period.



13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24 41. This facility’s purpose is to provide electronic communications across devices,  
25 including by communicating with Apple’s iCloud, an electronic communications service that  
26 electronically stores and maintains electronic information for iCloud users across various Apple  
27 devices.  
28

1           42.     The Universal Clipboard sends and receives electronic communications to one or  
2 more devices using BLE, authenticates each discovered device using iCloud, and temporarily  
3 stores and retrieves information transmitted to and from each device’s system clipboard.

4           43.     Specifically, the Universal Clipboard allows information—including  
5 communications—copied and cut on a first continuity-enabled Apple device (*e.g.*, iPhone, iPad,  
6 or Mac), to remain in a memory location on both the first continuity-enabled Apple device and one  
7 or more additional continuity-enabled Apple devices for a limited time, where the information can  
8 be accessed across applications by the user through a paste command.

9           44.     As Apple explains on its support page:

10                   With Universal Clipboard, you can copy text, images, photos, and  
11                   videos on one Apple device and then paste the content on another  
12                   Apple device. For example, you can copy a recipe from your Mac  
13                   and paste it into a note on your nearby iPhone. Or copy a file from  
14                   one Mac to paste in a folder on another Mac.

15           45.     Importantly, Apple is clear that the information is accessible when it is *pasted* by  
16 the user to a specified app or location.

17           46.     Indeed, Apple provides detailed instructions as to how Universal Clipboard is  
18 supposed to work:

- 19                   • Copy on a device: Select the content you want to copy, then  
20                   copy it. For example, on your Mac, press Command-C or  
21                   choose Edit > Copy.

22                   The copied content is available to paste on your other  
23 devices only for a short time.

- 24                   • Paste on a device: Position the pointer where you want to  
25                   paste the content, then paste it. For example, on your iPad,  
26                   double tap, then choose Paste from the options.

27           47.     The Universal Clipboard operates both as a conventional clipboard, allowing copy,  
28 cut and pasting functionality across applications on the same device, as well as a cross-device  
clipboard. That is, the Universal Clipboard ensures that information and communications copied  
by a user are temporarily stored, then seamlessly transmitted to nearby continuity-capable Apple  
devices.

1 48. A continuity-capable Apple device (*e.g.*, iPhone, iPad, or Mac) retrieves  
2 information from the Universal Clipboard when a user affirmatively pastes to a designated  
3 application or location, and in the case of the cross-device clipboard, when the user affirmatively  
4 pastes on a different device within a 120-second time period.

5 49. If nothing is pasted from the Universal Clipboard within 120 seconds of a copy  
6 command (which places information in the Universal Clipboard facility and pushes it to nearby  
7 continuity-capable devices), the transmitted contents of the Universal Clipboard are destroyed in  
8 all destination devices—but the copied information remains on the local clipboard of the device  
9 where it originated (*i.e.*, was copied).

10 50. If, however, a paste command is entered on a destination device within 120 seconds  
11 of Universal Clipboard transmission, the contents of the Universal Clipboard are stored on that  
12 destination device’s *local* clipboard—and become accessible on the destination device without any  
13 time limit.

#### 14 **IV. UNIVERSAL CLIPBOARD, ELECTRONIC COMMUNICATIONS, AND THE** 15 **UNDERSTANDING AND EXPECTATION OF PRIVACY**

16 51. The Universal Clipboard is designed to work out of the box with apps on iOS and  
17 MacOS devices. Namely, applications such as Calendar, Contacts, Mail, Messages, Notes, and  
18 Safari are all configured to use Handoff and the Universal Clipboard by default.

19 52. The information pasted to, from, and within these applications is thus  
20 predominantly the contents of electronic communications. For example, in the Messages app, a  
21 user can copy an image sent by another user and paste that image into a message to a different  
22 user. Indeed, virtually any form of electronic communication can be stored in a device clipboard,  
23 including audio recordings, general files, videos, photos, text messages, and medical information.

24 53. With respect to the Safari web browser, users obtain information from web servers  
25 through Hypertext Transfer Protocol (“HTTP”) or the secure, encrypted version of the protocol  
26 Hypertext Transfer Protocol Secure (“HTTPS”) requests.

27 54. Private information is often sent and received through HTTPS. The contents of the  
28 requests, including requests to POST and GET information are encrypted to prevent interception.

1 A person accessing a secure website, such as an online banking portal or their webmail, will do so  
2 through HTTPS, with all of the information sent to or from the HTTPS server encrypted. This  
3 prevents a third-party listening in on the transfer from reading the contents of the requests made  
4 to the web server and the potentially private contents returned from the web server.

5 55. Users frequently copy and paste information while working in their web browser.  
6 For example, a user may copy something from an e-mail displayed in their Gmail webmail and  
7 paste that information into another e-mail message.

8 56. When a user does this, the information is placed into the Universal Clipboard,  
9 where it remains until it is overwritten. Moreover, the information in the Universal Clipboard is  
10 accessible to nearby Apple devices for 120 seconds if those devices have Bluetooth enabled and  
11 are logged into Apple's iCloud servers.

12 57. In the case of material copied or cut into the Universal Clipboard from a webpage,  
13 particularly a secure webpage, the user does not expect that the unencrypted contents of his  
14 communications with the secure site will be accessible by others, including other applications or  
15 apps on nearby mobile devices.

16 58. The same is true for information copied or cut to the Universal Clipboard from an  
17 e-mail client, from Apple's Messages app, or from any other app primarily directed towards  
18 sending, receiving, and displaying electronic communications.

19 59. A user expresses his or her intent—and consent—to access the information in the  
20 Universal Clipboard is by entering a paste command. Users do not reasonably expect that the  
21 contents of their clipboard (particularly when the clipboard contains personal electronic  
22 communications, voice recordings, photos, passwords, cryptographic keys, and the like) to be  
23 accessible by other applications or devices unless and until the user herself enters a paste  
24 command.

25 60. The user thus has a reasonable expectation of privacy in the contents of her  
26 clipboard. For example, a user would not, and reasonably should not, expect that information that  
27 is, for example, encrypted in transit to a web server (such as for information copied from a secure  
28

1 site in Safari) will be autonomously accessed—in unencrypted form, no less—by other  
2 applications if the user copies that information into her device’s clipboard for her own later use.

3 61. Moreover, a user who copies the contents of an e-mail message on her Mac or iPad  
4 does not, and reasonably should not, expect that the contents of that message will, without user  
5 intervention, be accessed by apps on her iPhone. A reasonable iPhone, iPad, or Mac user expects,  
6 and reasonably should expect, that only apps (whether local or on a Handoff device) that  
7 affirmatively receive a paste command from the user will receive the information she has placed  
8 in the Universal Clipboard or on her own local clipboard.

9 62. A user’s paste command is unmistakable on most devices. For example, on iOS-  
10 touch-based devices, Apple has carefully defined gestures and interactions to ensure that a user  
11 has expressed her intent to copy, cut, or paste information to the Universal Clipboard. As Apple  
12 explains on its support site:

13 **Copy, cut, or paste**

- 14 • Copy: Pinch closed with three fingers.
- 15 • Cut: Pinch closed with three fingers two times.
- 16 • Paste: Pinch open with three fingers.

17 You can also touch and hold a selection, then tap Cut, Copy, or  
18 Paste.

19 63. These complex gestures are designed to require a deliberate act by the user, and this  
20 is not an accident. The design ensures that information is placed in, and read from, a user’s  
21 Universal Clipboard and local device clipboard *only* when the *user* intends to do so.

22 64. This is because for most users, including Plaintiff, the Universal Clipboard  
23 routinely and frequently stores a wide range of highly sensitive information on a temporary basis.  
24 For example, users routinely store medical information, passwords, cryptographic tokens, text  
25 message contents, private and personal photos, and the contents of e-mails in the Universal  
26 Clipboard for temporary storage and retrieval.

27 65. The most common use cases for users, including for Plaintiff, are the copying and  
28 pasting of images, files, and text from web browsers (including from secure webpages), messaging

1 apps, or the system file browser (*e.g.*, the Finder). During the course of a day, a user (including  
2 Plaintiff) copies and pastes electronic communications on an iPhone or computer countless times.  
3 This is all done with the expectation that what the user places in the Universal Clipboard is  
4 accessible when the user wants that information—but only at the user’s consent and command  
5 through a user-initiated paste command.

6 66. An example of a common use case by Apple device users, including Plaintiff, is a  
7 photo received as part of a text message. An iPhone or iPad user will frequently copy the text or  
8 image in an iMessage and resend it to another user in another text message or e-mail. The user  
9 expects, and reasonably should expect, that the copied image will be accessible only by her—and  
10 only when she indicates that the information should be pasted. No reasonable user expects that a  
11 photo temporarily copied into the clipboard on an iPhone will be autonomously accessed and used  
12 by other applications on that iPhone—let alone applications on another Apple device.

13 67. Put simply, clipboards generally, and the Universal Clipboard specifically, are  
14 meant to allow a user to store and receive information in a temporary space in memory. The only  
15 person expected to access that information is the user. Users do not, and reasonably should not,  
16 expect that electronic communications—including the substance of e-mails, messages, photos, and  
17 other communications—will be autonomously read by any apps residing on nearby Apple devices,  
18 nor do they expect that the contents of nearby Apple devices’ clipboards will be read by apps on  
19 their local device without an affirmative paste command by the user.

20 **V. LINKEDIN’S IOS APP REPEATEDLY READS THE CONTENTS OF THE**  
21 **UNIVERSAL CLIPBOARD WITHOUT USER PERMISSION.**

22 68. Millions of users access the LinkedIn social network through a native app on their  
23 iPhones and iPads, the LinkedIn App. Indeed, approximately 57% of LinkedIn’s traffic comes  
24 from mobile devices.

25 69. The LinkedIn App is programmed to enable social interactions on a network,  
26 facilitate communications with other users, including through messages, and to allow the user to  
27 read and write LinkedIn posts.  
28

1           70.     In 2019, LinkedIn generated \$6.8 billion in revenue. The company made money on  
2 premium subscriptions as well as by selling advertising targeting its users. According to estimates,  
3 LinkedIn’s users are each worth \$78.27 to the company. Moreover, the average revenue per user  
4 on LinkedIn is \$3.21.

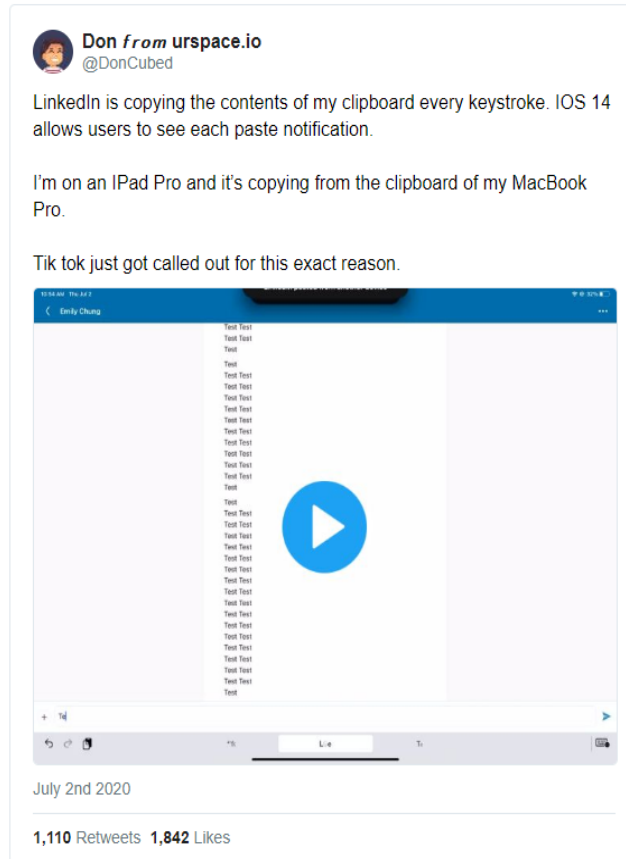
5           71.     The LinkedIn App is developed by LinkedIn and distributed on Apple’s App Store  
6 for iOS devices, including the iPhone and iPad, which are some of the most popular mobile and  
7 touch-enabled devices in the United States.

8           72.     In early 2020, Apple began beta-testing its newest iOS operating system release:  
9 iOS 14. One new feature introduced in iOS 14 is the ability to configure the operating system to  
10 provide a notification each time data is “pasted” from the system clipboard or the Universal  
11 Clipboard.

12           73.     Developers and other iOS 14 beta testers who enabled this feature discovered for  
13 the first time that the LinkedIn App for the iPhone and iPad was frequently reading from the  
14 Universal Clipboard and system clipboard and “pasting” its contents without the user’s permission,  
15 *i.e.*, even when the user had never entered a paste command on a device or in the LinkedIn App.

16           74.     As one user on twitter, @DonCubed, noted on or around July 2nd, 2020, LinkedIn  
17 was reading from the Universal Clipboard after every keystroke on the LinkedIn App without  
18 users’ knowledge or permission. If not for the new clipboard notification in iOS 14, LinkedIn App  
19 users, including Plaintiff, would never have known that the contents of their Universal Clipboard  
20 was being read repeatedly by LinkedIn and used by the LinkedIn iOS App.

1           75.     @DonCubed also discovered that the information in his Universal Clipboard was  
2 being copied from the clipboard of his MacBook Pro to his nearby mobile device. He posted a  
3 video demonstrating the repeated, involuntary reading by LinkedIn from his Universal Clipboard  
4 and system clipboard, including from information stored across different devices.



20           76.     A LinkedIn senior executive and engineer acknowledged this behavior by  
21 LinkedIn's App and confirmed that the LinkedIn iOS App's code was written to repeatedly read  
22 the contents of the Universal Clipboard and system clipboard, including to compare the clipboard  
23 contents to what is typed into a text box in the LinkedIn App.

24           77.     This behavior requires extensive interaction with the iPhone and iPad application  
25 programming interfaces ("APIs") in iOS. The Universal Clipboard and system clipboard cannot be  
26 accessed inadvertently—an app must be coded to specifically read from a clipboard (sometimes  
27 referred to as a pasteboard).

28



1           78.     Indeed, the Universal Clipboard is integrated with the general system clipboard /  
2 pasteboard on Apple devices. As Apple explains in its documentation for the NSPasteboard object,  
3 interactions with the general pasteboard automatically work with the Universal Clipboard:

4                     The general pasteboard, available by way of the general class  
5                     method, automatically participates with the Universal Clipboard  
6                     feature in macOS 10.12 and later and in iOS 10.0 and later. There is  
7                     no macOS API for interacting with this feature.

8           79.     This documentation makes clear that by interacting with the operating system’s  
9 general pasteboard, LinkedIn not only knew it was reading information placed in the clipboard by  
10 the user for his own purposes, but also that the contents of the Universal Clipboard would be  
11 transferred to and from nearby devices as part of the Universal Clipboard and Continuity  
12 subsystems.

13           80.     Indeed, LinkedIn reads from the Universal Clipboard contemporaneously with the  
14 transfer of the same information to other nearby devices. The Universal Clipboard’s contents are  
15 stored in a subsystem in iOS that allocates memory storage to hold information cut or copied to  
16 the clipboard. That subsystem then transmits the contents of the Universal Clipboard to nearby  
17 devices through a facility capable of sending and receiving electronic communications using BLE  
18 and authenticating / identifying the nearby devices using Apple’s iCloud service.

19           81.     By repeatedly reading from the Universal Clipboard, the LinkedIn App ensures that  
20 it can read the contents of the Universal Clipboard prior to, or contemporaneously with, the  
21 transmission from nearby devices.

22           82.     For example, if a user has the LinkedIn App open on his iPhone and walks within  
23 BLE range of a nearby Macintosh computer, the contents of the Macintosh computer’s clipboard  
24 are transferred to the iPhone—where the LinkedIn App immediately and surreptitiously reads it at  
25 the first user keystroke.

26           83.     Because the data transferred through the Universal Clipboard expires on remote  
27 devices after 120 seconds, the LinkedIn App is designed to circumvent the timer by reading the  
28 contents of the Universal Clipboard upon every keystroke in the LinkedIn App. The act of reading  
the contents of the Universal Clipboard is understood by iOS as a “paste” command, no different

1 than one that would be normally issued by a user. Once that command is triggered by LinkedIn,  
2 the information pulled from the Universal Clipboard becomes permanent on the remote device.

3 84. In the case above, (a) the iPhone running the LinkedIn iOS App comes within range  
4 of a Macintosh with private information in the Macintosh's local clipboard; (b) the information in  
5 the Macintosh's clipboard is transmitted, upon authentication through iCloud, to the iPhone, and  
6 (c) the LinkedIn iOS App on the iPhone immediately reads the contents of the Universal Clipboard,  
7 making that information permanent on the iPhone, which in turn means that the information can  
8 be accessed by LinkedIn and other apps on the iPhone even after the 120 seconds have expired.

9 85. This repeated reading is unmistakably intentional, as it has the effect of  
10 circumventing the automatic deletion of Universal Clipboard contents pushed to remote devices.

11 86. As another example, if an iPhone running LinkedIn stores information in its local  
12 clipboard, that information is immediately captured and intercepted by the LinkedIn App (when  
13 the user enters keystrokes) as it is transferred via Universal Clipboard to nearby devices.

14 87. This frequent interception of personal and private information in device clipboards  
15 is highly invasive. Indeed, users, including Plaintiff, routinely copy or cut electronic  
16 communications, including personal information from messages and e-mails, into the Universal  
17 Clipboard. They do not expect that LinkedIn is reading this information unless they expressly paste  
18 that information into the LinkedIn App.

19 88. Plaintiff and the Class Members never authorized LinkedIn to receive, access, or  
20 intercept the data that the LinkedIn App accessed and copied. LinkedIn's iOS users, including  
21 Plaintiffs and the Class Members were not informed that LinkedIn has repeatedly accessed the  
22 contents of their Universal Clipboard, including electronic communications stored there, without  
23 authorization.

24 89. Moreover, LinkedIn never disclosed in any user agreement or public website that  
25 it reads the contents of user clipboards, including electronic communications cut or copied to the  
26 Universal Clipboard. It did so in secret.

**CLASS ACTION ALLEGATIONS**

**The Nationwide LinkedIn App User Class**

90. Plaintiff brings this nationwide class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following Class:

All natural-person LinkedIn users who installed and used the LinkedIn App within the United States from September 13, 2016 (or the earliest date LinkedIn began reading from device clipboards without consent) until the present (the “Class Period”), or in the alternative, until the date upon which LinkedIn ceased or ceases accessing electronic communications and information in the Apple Universal Clipboard without notification and consent.

91. Excluded from the Class are the following individuals and/or entities: LinkedIn and its parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which LinkedIn has a controlling interest; counsel for the putative class and their immediate family members; and all judges and court staff assigned to hear or administer any aspect of this litigation, as well as their immediate family members.

**The Nationwide Continuity Class**

92. Plaintiff brings this nationwide class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following Class:

All natural-person LinkedIn users of the LinkedIn App who own and actively use at least two continuity-capable Apple devices, and installed and used the LinkedIn App within the United States from September 13, 2016 (or the earliest date LinkedIn began reading from device clipboards without consent) until the present (the “Class Period), or in the alternative, until the date upon which LinkedIn ceased or ceases accessing electronic communications and information in the Apple Universal Clipboard without notification and consent.

93. Plaintiffs reserve the right to modify or amend the definition of the proposed Classes before the Court determines whether certification is appropriate. Unless stated otherwise, for example with respect to a particular count, members of either or both classes are referred to in this Complaint as the Class Members.

1 **Numerosity and Ascertainability**

2 94. The Classes are so numerous that joinder of all members is impracticable. On  
3 information and belief there are more than 160 million LinkedIn users in the United States, millions  
4 of whom have used the LinkedIn App and have been injured by the conduct alleged herein. The  
5 likely millions of members of the putative class are identifiable and ascertainable based on  
6 LinkedIn's records.

7 95. Plaintiffs anticipate providing appropriate notice to the certified Classes, in  
8 compliance with Fed. R. Civ. P. 23(c)(1)(2)(A) and/or (B), to be approved by the Court after class  
9 certification, or pursuant to court order under Fed. R. Civ. P. 23(d).

10 **Predominance of Common Issues**

11 96. This action satisfied the requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3)  
12 because questions of law and fact that have common answers that are the same for the Classes  
13 predominate over questions affecting only individual Class members. These include, without  
14 limitation, the following:

15 a. Whether LinkedIn intentionally intercepted, endeavored to intercept, or  
16 procured any other person to intercept or endeavor to intercept Plaintiff's and the Class  
17 Members' electronic communications from the Universal Clipboard.

18 b. Whether LinkedIn intentionally accessed, endeavored to access, or  
19 procured any other person to access or endeavor to access Plaintiff's and the Class Members'  
20 Universal Clipboards.

21 c. Whether LinkedIn had authorization to intercept or access Plaintiff's and  
22 the Class Members' Universal Clipboards and communications from Plaintiff's and the Class  
23 Members' Universal Clipboards.

24 d. The amount of statutory damages that should be levied against LinkedIn.

25 e. Whether LinkedIn should be enjoined from its violations of the Electronic  
26 Communications Privacy Act and the Stored Communications Act.

27 f. Whether LinkedIn's conduct was unlawful.  
28

1 **Typicality**

2 97. This action satisfies the requirements of Fed. R. Civ. P. 23(a)(3) because Plaintiff's  
3 claims are typical of the claims of other Class members and arise from the same course of conduct  
4 by Defendant LinkedIn. The relief Plaintiffs seek is typical of the relief sought for the absent Class  
5 members.

6 **Adequate Representation**

7 98. Plaintiff will fairly and adequately represent and protect the interests of the Classes.  
8 Plaintiff has retained counsel with substantial experience in prosecuting consumer class actions,  
9 including actions involving the unauthorized access of sensitive, personal information.

10 99. Plaintiff and his counsel are committed to vigorously prosecuting this action on  
11 behalf of the Classes and have the financial resources to do so. Neither Plaintiff nor his counsel  
12 have interests adverse to those of the Class.

13 **Superiority**

14 100. This action satisfies the requirements of Fed. R. Civ. P. 23(b)(2) because Defendant  
15 LinkedIn has acted and refused to act on grounds generally applicable to the Classes, thereby  
16 making appropriate final injunctive and/or corresponding declaratory relief with respect to each  
17 Class as a whole.

18 101. This action satisfies the requirements of Fed. R. Civ. P. 23(b)(3) because a class  
19 action is superior to other available methods for the fair and efficient adjudication of this  
20 controversy. The common questions of law and fact regarding Defendant LinkedIn and  
21 responsibility predominate over any question affecting only individual Class members.

22 102. Because the damages suffered by each individual Class member may be relatively  
23 small, the expense and burden of individual litigation would make it very difficult or impossible  
24 for individual Class members to redress the wrongs done to each of them individually, such that  
25 most or all Class members would have no rational economic interest in individually controlling  
26 the prosecution of specific actions, and the burden imposed on the judicial system by individual  
27 litigation by even a small fraction of the Class would be enormous, making class adjudication the  
28 superior alternative under Fed. R. Civ. P. 23(b)(3)(A).



1           108. For example, version 9.1.183 of the LinkedIn App, released in late June 2020,  
2 performs as follows in normal operation:

- 3           • When the LinkedIn App is in the foreground of an iPhone or iPad, LinkedIn  
4 deliberately and repeatedly accesses the clipboard—including the Universal  
5 Clipboard, if available—with each keystroke in the app. That is, every time a  
6 user of the LinkedIn App (1) types into the search bar; (2) writes a post (or  
7 comments on another’s post); (3) writes or responds to a LinkedIn message;  
8 (4) creates or edits their LinkedIn profile; (5) applies for a job; or (6) does  
9 anything else that involves entering a *single typed character*, LinkedIn reads  
10 the user’s clipboard.
- 11           • LinkedIn does not tell users it is reading their clipboard. It does not ask users  
12 for their permission to read their clipboard. And it does not disclose *anywhere*  
13 that the LinkedIn App is constantly reading an iPhone or iPad user’s  
14 clipboard—not just from that device, but from *other Apple devices, including*  
15 *Mac computers*, in the room with that particular iPhone or iPad.
- 16           • Nonetheless, the LinkedIn App is constantly reading a user’s clipboard—from  
17 the device on which the App is running, and from other nearby Apple devices  
18 and computers signed in with the same Apple ID. And when the LinkedIn  
19 App—without a user’s knowledge or permission—reads that user’s Universal  
20 Clipboard, it *changes things*. Most egregiously, when the LinkedIn App on an  
21 iPhone or iPad reads a user’s Universal Clipboard, this secret behavior *changes*  
22 *the contents of the user’s on-device clipboard, thereby circumventing Apple’s*  
23 *security-critical timeout limitation on Universal Clipboard persistence*.

24           109. Thus, even though Apple designed its continuity system from the ground up to  
25 ensure that information copied on one Apple device (for example, a user’s MacBook) would not  
26 sit *indefinitely* on the local clipboard of a *different* Apple device (for example, that user’s  
27 iPhone)—a basic privacy and security expectation of consumers and system architects alike—  
28 LinkedIn intentionally built its App to circumvent this protection.

1           110. In performing the above and related behaviors through its LinkedIn App version  
2 9.1.183 (and predecessor versions stretching back perhaps as early as 2016), LinkedIn violates at  
3 least subsections (a) and (d) of 18 U.S.C. § 2511.<sup>1</sup>

4           111. For example, LinkedIn intentionally intercepts an electronic communication  
5 through the normal behavior of its LinkedIn App version 9.1.183 (and similarly-coded predecessor  
6 versions) in at least the following common use cases:

- 7           • When a person is using the LinkedIn App on their iPhone or iPad (here, the  
8 “LinkedIn iOS Device”) and a copy command is entered on a nearby continuity-  
9 enabled Apple device (e.g., a Macintosh computer, iPhone, or iPad signed into  
10 the same Apple ID), the information copied on the continuity-enabled Apple  
11 device is pushed via a Continuity Subsystem to temporary storage on the  
12 LinkedIn iOS Device. Without the user’s knowledge or approval, the LinkedIn  
13 App intercepts the pushed information through a surreptitious clipboard read  
14 upon the first active keystroke by a LinkedIn App user (e.g., text entry into a  
15 search bar; a message box; a post or status update; or other LinkedIn App  
16 keystroke). Upon the LinkedIn App’s intercept of the pushed information from  
17 the separate continuity-enabled Apple device, the 120-second timer limiting the  
18 persistence of that information on the LinkedIn iOS Device is destroyed without  
19 the user’s knowledge or consent. Thereafter, the LinkedIn App—and any other  
20 applications on the LinkedIn iOS App that may later be used before a new item  
21 is copied to the clipboard—may use, disclose, or otherwise access the  
22 intercepted information at their leisure, *without the LinkedIn App user ever*  
23 *realizing that information copied on a different Apple device has covertly*  
24 *been intercepted and redirected to a persistent, local clipboard on the*  
25 *LinkedIn iOS Device.*

---

26  
27           <sup>1</sup> Plaintiff has reason to believe, but has not yet confirmed, that LinkedIn also violates  
28 subsection (c) by intentionally disclosing, or endeavoring to disclose, the contents of the electronic  
communications it intercepts from the Continuity / Universal Clipboard subsystem.



- When a person is using the LinkedIn App on their iPhone or iPad (again, the “LinkedIn iOS Device”) and they enter BLE range of a continuity-enabled Apple device (e.g., a Macintosh computer, iPhone, or iPad signed into the same Apple ID), any information in the LinkedIn iOS Device’s Universal Clipboard is pushed via a Continuity Subsystem to the continuity-enabled Apple device. Without the user’s knowledge or approval, the LinkedIn App intercepts this pushed information through a surreptitious clipboard read upon the next active keystroke by a LinkedIn App user (e.g., text entry into a search bar; a message box; a post or status update; or other LinkedIn App keystroke).

112. In each of the above use cases, LinkedIn, through the LinkedIn App, intentionally intercepts an electronic communication. For example, as described above, the LinkedIn App uses repeated pasteboard (*i.e.*, Universal Clipboard) reads to contemporaneously intercept (i) inbound electronic communications to the LinkedIn iOS Device (information copied on, then electronically pushed from, a separate Apple continuity device), as described in the first exemplary use case; and (ii) outbound electronic communications from the LinkedIn iOS Device (information copied on the LinkedIn iOS Device, then electronically pushed to a separate Apple continuity device), as described in the second exemplary use case.

113. In each of the exemplary use cases, LinkedIn’s interception is intentional. For example, the LinkedIn App includes—as admitted by LinkedIn’s own executive—one or more specific code paths expressly written to perform the electronic interception (performed via surreptitious clipboard reads) described in each exemplary use case.

114. In each of the exemplary use cases, LinkedIn intentionally uses, or endeavors to use, the contents an electronic communication, knowing or having reason to know that the information was obtained through interception of an electronic communication in violation of 18 U.S.C. § 2510 *et seq.*

115. For example, for each “read” of the Universal Clipboard performed by the LinkedIn App in the exemplary use cases, LinkedIn performs a “compare” on the contents of the intercepted communication. As with all other aspects of LinkedIn’s surreptitious abuse of Apple’s Universal

1 Clipboard and continuity functionality, the “compare” function (*i.e.*, LinkedIn’s use of intercepted  
2 electronic communications) is intentional, performed by purpose-built computer code in the  
3 LinkedIn App. Additionally, by executing compares repeatedly in connection with clipboard reads  
4 whenever the LinkedIn App is active on a LinkedIn iOS Device, LinkedIn uses information it  
5 knows or should know has been obtained through unlawful interception of content from Apple’s  
6 Universal Clipboard. Indeed, the clipboard read-and-compare functionality in the LinkedIn App  
7 appears to be specifically designed for such unlawful interception and use.

8       116. In each of the exemplary use cases, LinkedIn’s actions affect interstate commerce.  
9 For example, LinkedIn’s surreptitious activity intercepts, uses, and redirects information  
10 electronically communicated through a Continuity Subsystem specifically designed by Apple to  
11 require multilateral network authentication to an Apple ID auth server and wireless data  
12 transmission between authenticated devices, which subsystem is integral to secure, private use of  
13 personal electronic devices by tens of millions of Americans—and millions of LinkedIn App users  
14 like Plaintiff and the proposed class.

15       117. Each of the exemplary use cases is commonplace among LinkedIn App users with  
16 at least two continuity-enabled Apple devices (*e.g.*, an iPhone and a Mac; an iPhone and an iPad;  
17 an iPad and a Mac; and various combinations and aggregations of the foregoing). Plaintiff is such  
18 a LinkedIn App user, as are members of the proposed class.

19       118. For example, Plaintiff is an active user of the LinkedIn App and owns and uses  
20 multiple Continuity-enabled Apple devices that share a Universal Clipboard. When Plaintiff uses  
21 his LinkedIn App contemporaneously with his MacBook or his other continuity-enabled Apple  
22 devices (*e.g.*, iPad), he suffers electronic interception by LinkedIn as described in the first  
23 exemplary use case. When Plaintiff uses his LinkedIn App on his iPhone while walking around  
24 (thereby entering in and out of BLE range of his MacBook and his other continuity-enabled Apple  
25 devices (*e.g.*, iPad)), he suffers electronic interception by LinkedIn as described in the second  
26 exemplary use case. Plaintiff is representative of the proposed class of LinkedIn App users who  
27 own at least two continuity-enabled Apple devices in both respects.  
28

1 119. The LinkedIn actions described above—including the LinkedIn App’s surreptitious  
2 interception of electronic Universal Clipboard communications as described in the exemplary use  
3 cases—are not necessary practices for providers of electronic communications, nor are they  
4 incidental to the act of facilitating electronic communications.

5 120. For each of the exemplary use cases, LinkedIn uses purpose-written computer code  
6 in the LinkedIn App to intercept electronic communications in Apple’s Universal Clipboard /  
7 Continuity Subsystem. LinkedIn’s intercepting technology is not used for the ability to send or  
8 receive Universal Clipboard / Continuity communications in either exemplary use case.

9 121. Plaintiff and Class Members have suffered harm and injury due to LinkedIn’s  
10 above-described unlawful interception and use of their private and personal, confidential, and  
11 sensitive communications on continuity-enabled Apple devices.

12 122. 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  
14 and 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 LinkedIn 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.

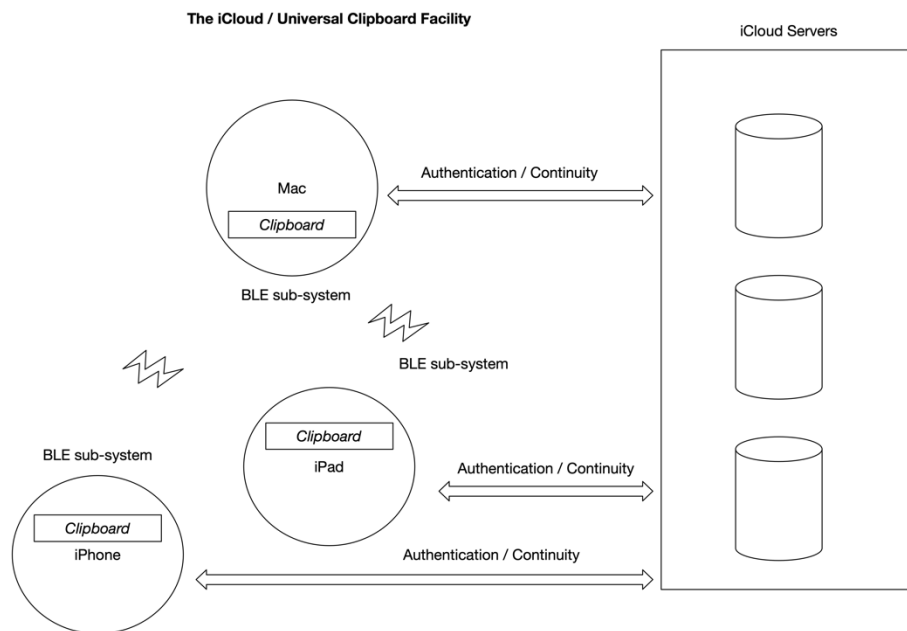
19 **COUNT TWO**  
20 **(on behalf of Plaintiff and the Continuity Class)**  
21 **THE STORED COMMUNICATIONS ACT**  
**(18 U.S.C. § 2701, *et seq.*)**

22 123. Plaintiff realleges and incorporates by reference all the preceding paragraphs and  
23 allegations of this Complaint as if fully set forth here.

24 124. Plaintiff, individually and on behalf of all Class Members, asserts violations of 18  
25 U.S.C. § 2701(a) for LinkedIn’s unlawful and unauthorized access of electronic  
26 communications—*i.e.*, inbound and outbound Universal Clipboard data—that are temporarily  
27 stored in the Universal Clipboard / Continuity Subsystem facility associated with these users’  
28

1 continuity-enabled Apple devices in connection with that data’s wireless transmission via the  
 2 cross-device Universal Clipboard.

3 125. The Universal Clipboard and Continuity Subsystem comprise a “facility” through  
 4 which an electronic communication service is provided within the meaning of 18 U.S.C.  
 5 § 2701(a)(1) and (2). The Universal Clipboard / Continuity Subsystem facility is a multi-device,  
 6



7  
 8  
 9  
 10  
 11  
 12  
 13  
 14  
 15  
 16 networked collection of hardware and software components (some local to Apple devices, some  
 17 in iCloud) that perform tightly integrated tasks to facilitate Apple’s cross-device Universal  
 18 Clipboard service—*e.g.*, secure cross-device authentication with a trusted authority (iCloud);  
 19 wireless transmission and temporary storage of copied information; and security / privacy  
 20 safeguards such as local timeouts on cross-device data. The Universal Clipboard / Continuity  
 21 Subsystem facility comprises: (a) the Apple iCloud service, which is used for authentication and  
 22 coordination among Apple devices and their clipboards; (b) the volatile memory on each Apple  
 23 device wherein local clipboard information is temporarily stored; and (c) the networking and BLE  
 24 subsystem components on each continuity-enabled Apple device. The Continuity Subsystem and  
 25 the Universal Clipboard work together to ensure the synchronization and transmission among  
 26 Apple devices with properly authenticated user credentials through Apple’s iCloud service. A  
 27 high-level diagram of the Universal Clipboard / Continuity Subsystem facility appears below.  
 28

1           126. As described in Count One and in the Facts section of this Complaint, LinkedIn,  
2 via regular operation of its LinkedIn App version 9.1.183 (and many predecessor versions)  
3 intentionally accesses information temporarily stored for transmission via Apple’s cross-device  
4 Universal Clipboard and Continuity Subsystem—sensitive information associated with, and  
5 private to, Plaintiff and Class Members. For example, in each exemplary use case set forth in Count  
6 One, LinkedIn intentionally accesses such temporarily-stored information. LinkedIn’s access to  
7 this information is unauthorized—indeed, it is done surreptitiously without notice to, or consent  
8 from, Plaintiff or Class Members, is done contrary to expected (reasonably so) application  
9 behavior, and circumvents system-level security and privacy safeguards Apple itself has built into  
10 its Universal Clipboard / Continuity Subsystem facility (*e.g.*, a 120-second timeout on cross-device  
11 Universal Clipboard persistence). In short, for at least the exemplary use cases outlined in Count  
12 One, LinkedIn intentionally accesses, and has intentionally accessed, without authorization a  
13 facility through which an electronic communication service is provided in violation of 18 U.S.C.  
14 § 2701(a)(1).

15           127. Moreover, by accessing the contents of the Universal Clipboard without notice to,  
16 or consent from, Plaintiff and Members of the Class, LinkedIn intentionally exceeded an  
17 authorization to access a facility through which an electronic communication service is provided  
18 in violation of 18 U.S.C. § 2701(a)(2). As noted above, for each exemplary use case, LinkedIn’s  
19 access to the Universal Clipboard / Continuity Subsystem facility intentionally exceeds an  
20 authorization: LinkedIn accesses the Universal Clipboard / Continuity Subsystem facility  
21 surreptitiously, without notice to or consent from Plaintiff or Class Members (whose data LinkedIn  
22 is accessing from that facility); the LinkedIn App’s behavior to access this facility is done contrary  
23 to reasonably expected application behavior in a computer or mobile device; and LinkedIn’s access  
24 deliberately circumvents system-level security and privacy safeguards Apple itself has built into  
25 its Universal Clipboard / Continuity Subsystem facility (*e.g.*, a 120-second timeout on cross-device  
26 Universal Clipboard persistence).

27           128. LinkedIn’s actions in accessing the Universal Clipboard / Continuity Subsystem  
28 facility affect interstate commerce. For example, LinkedIn’s surreptitious activity intercepts, uses,

1 and redirects information electronically communicated through a Continuity Subsystem  
2 specifically designed by Apple to require multilateral network authentication to an Apple ID auth  
3 server and wireless data transmission between authenticated devices, which subsystem is integral  
4 to secure, private use of personal electronic devices by tens of millions of Americans—and  
5 millions of LinkedIn App users like Plaintiff and the proposed class.

6 129. LinkedIn, through its LinkedIn App, repeatedly retrieves information stored and  
7 synchronized among a network of nearby continuity-enabled Apple devices without authorization  
8 by reading, without notice to, or consent from, users—including Plaintiff and Class Members—  
9 the contents of the cross-device Universal Clipboard and the local system clipboard on individual  
10 devices.

11 130. LinkedIn, through normal operation of its LinkedIn App, intentionally obtains and  
12 alters a wire or electronic communication while it is in electronic storage. For example, the  
13 information in each continuity-enabled Apple device’s local clipboard is stored temporarily in a  
14 subsystem before it is pushed to nearby continuity-enabled Apple devices as part of the cross-  
15 device Universal Clipboard. The LinkedIn App reads and uses this information. Additionally, the  
16 LinkedIn App reads and uses information stored and synchronized across multiple continuity-  
17 enabled Apple devices through the Universal Clipboard / Continuity Subsystem facility, and in  
18 doing so obtains and alters a wire or electronic communication while it is in electronic storage.

19 131. Because the LinkedIn App repeatedly issues surreptitious “paste” commands  
20 without informing or asking for consent from users, LinkedIn makes the temporarily stored  
21 information in the cross-device Universal Clipboard permanent on the local device on which the  
22 LinkedIn App runs, circumventing Apple’s 120-second expiration timer for the information stored  
23 and synchronized as part of the Universal Clipboard. This is an intentional act, designed to allow  
24 unfettered, unauthorized, and unreasonable access by a third-party iOS application (the LinkedIn  
25 App) to sensitive clipboard contents on nearby Apple devices.

26 132. The LinkedIn App repeatedly and continuously reads information from the local  
27 device clipboard and the cross-device Universal Clipboard because it was intentionally  
28 programmed to do so by LinkedIn. Indeed, programming the LinkedIn App to perform in the

1 manner described in this Count requires the intentional writing, testing, debugging, and  
2 deployment of purpose-built computer software code, including the use of Apple iOS application  
3 programming interfaces.

4 133. The information read and used by the LinkedIn App constitutes and “Electronic  
5 communication” because it involves the transfer of signs, signals, writing, images, sounds, data,  
6 or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic,  
7 photoelectric or photooptical system that effects interstate or foreign commerce. 18 U.S.C.  
8 § 2510(12). The information read from system clipboards and the Universal Clipboards includes  
9 pictures, texts, files and other objects. Moreover, the information is transmitted to and from the  
10 Universal Clipboard through electromagnetic, wire, and radio transmissions—namely using  
11 wireless networks, including BLE and WiFi. The electronic communications in question—and the  
12 sensitive pictures, texts, files, and other objects described here—are those of Plaintiff and Class  
13 Members. LinkedIn’s access and use of these communications is indisputably unauthorized by  
14 Plaintiff and Class Members—who among other things definitionally have not entered a user-  
15 generated “paste” command in either of the exemplary use cases, or during any other aspect of the  
16 LinkedIn App’s clipboard-abusing behavior.

17 134. The Continuity Subsystem and the Universal Clipboard, which together comprise  
18 a facility for the transmission of electronic communication, only perform in conjunction with  
19 Apple’s iCloud electronic communication service, such that the synchronization of information  
20 among Apple devices indisputably employs the instrumentalities of interstate commerce and  
21 affects interstate commerce.

22 135. LinkedIn’s actions described in this Count are not necessary practices for providers  
23 of electronic communications, nor are they incidental to the act of facilitating electronic  
24 communications.

25 136. The LinkedIn App’s continuous reading of the system clipboards and the Universal  
26 Clipboard is not part of the intended use of the LinkedIn App. Moreover, no part of the User or  
27 Privacy Agreement between Plaintiff (or the Class Members) and LinkedIn discloses any use or  
28 action by LinkedIn involving the contents of user clipboards.

1 137. As a result of LinkedIn’s violations of the Stored Communications Act, Plaintiff  
2 and Class Members have suffered harm and injury, including but not limited to the invasion of  
3 their privacy rights, due to the unauthorized disclosure of private and personal, confidential, and  
4 sensitive communications.

5 138. Pursuant to 18 U.S.C. § 2707, Plaintiffs and Class Members are entitled to:  
6 (1) appropriate equitable or declaratory relief; (2) damages, in an amount to be determined at trial,  
7 assessed as the sum of the actual damages suffered by Plaintiffs and Class Members, and any  
8 profits made by LinkedIn as a result of the violation, but in no case less than the minimum statutory  
9 damages of \$1,000 per person; and (3) reasonable attorneys’ fees and other litigation costs  
10 reasonably incurred.

11 **COUNT THREE**  
12 **(on behalf of Plaintiff and the Nationwide LinkedIn App User Class)**  
13 **Intrusion Upon Seclusion**

14 139. Plaintiff realleges and incorporates by reference all the preceding paragraphs and  
15 allegations of this Complaint as if fully set forth here.

16 140. LinkedIn, through normal operation of the LinkedIn App, intrudes upon and has  
17 intruded upon the seclusion of Plaintiff and Class Members. For example, version 9.1.183 of the  
18 LinkedIn App—and many prior versions dating back potentially several years—have, in their  
19 normal operation, facilitated LinkedIn’s intentional intrusion into places, conversations, and  
20 matters as to which Plaintiff and Class Members had a reasonable expectation of privacy, and these  
21 intrusions were highly offensive to a reasonable person, as described below and throughout this  
22 Complaint.

23 141. As described in Counts One and Two and in the Facts section of this Complaint,  
24 LinkedIn uses and has used the LinkedIn App to intercept, record, transmit, and use Plaintiff’s and  
25 Class Members’ electronic communications from Apple’s Universal Clipboard without those  
26 persons’ knowledge or consent. This constitutes and has constituted an intentional intrusion upon  
27 the Plaintiff’s and Class Members’ solitude or seclusion in that LinkedIn effectively placed itself  
28 in the middle of a conversation to which it was not invited, welcomed, or authorized.



1           142. Plaintiff and Class Members did not consent to, authorize, or know about  
2 LinkedIn’s intrusion at the time occurred. Plaintiff and Class Members never agreed (nor even  
3 knew) that LinkedIn would—surreptitiously and without user direction such as a user-initiated  
4 paste command—repeatedly read and issue compare and paste commands to both local device  
5 clipboards and Apple’s cross-device Universal Clipboard.

6           143. Plaintiff and Class Members did not consent to the information in their local device  
7 clipboard or their cross-device Universal Clipboard being read without their permission or  
8 direction by LinkedIn. Indeed, nothing in any agreements Plaintiff or Class Members made with  
9 LinkedIn disclosed or even hinted that a user’s private information from other apps *and even other*  
10 *devices* would be repeatedly read, compared, and pasted by the LinkedIn App from a user’s local  
11 clipboard or cross-device Universal Clipboard without the user’s express direction (*e.g.*, through  
12 a user-initiated paste command).

13           144. LinkedIn’s intentional intrusion on Plaintiff’s and Class Members’ solitude and  
14 seclusion without consent would be highly offensive to a reasonable person. Plaintiff and Class  
15 Members reasonably expected, based on Apple and LinkedIn disclosures and a widespread,  
16 common understanding of how device clipboards (a longstanding staple of personal computing)  
17 work, that LinkedIn would not be autonomously reading and using the contents of a user’s  
18 clipboard—let alone repeatedly doing so, and reading clipboard information communicated *from*  
19 *other devices*—without a user-initiated paste command in the LinkedIn App.

20           145. LinkedIn’s intentional intrusion into Plaintiff and Class Members’ private  
21 conversations was further highly offensive to a reasonable person in that it violated federal and  
22 state laws designed to protect individual privacy.

23           146. LinkedIn’s surreptitious taking and use of personal, confidential, and private  
24 information from millions of individuals—including Plaintiff and Class Members—was highly  
25 offensive because it violated these users’ expectations of privacy that have been established by  
26 general social norms. Privacy polls and studies consistently show that the overwhelming majority  
27 of Americans believe one of the most important privacy rights is the need for an individual’s  
28 affirmative consent before personal data is harvested or shared. Plaintiff agrees.

1 147. As described in Counts One and Two and in the Facts section, LinkedIn  
2 intentionally engages in the privacy-harming misconduct alleged in this Complaint, including the  
3 misconduct that intrudes upon Plaintiff and Class Members' seclusion. Given LinkedIn's business  
4 model of directly and indirectly monetizing data, the complained-of actions by LinkedIn—  
5 including the LinkedIn App's near-constant, surreptitious information-mining of users' local and  
6 cross-device clipboards—are plainly intended to obtain additional data for LinkedIn's substantial  
7 profit, including, but not limited to, enhanced monetization of the LinkedIn App.

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

10 149. Unwanted access to data by electronic or other covert means, in violation of the law  
11 or social norms, is actionable under California law.

12 150. Plaintiff and the Class Members have been damaged as a direct and proximate result  
13 of LinkedIn's invasion of their privacy, and are entitled to just compensation.

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

18 **COUNT FOUR**  
19 **(on behalf of Plaintiff and the Nationwide LinkedIn App User Class)**  
20 **Invasion of Privacy**

21 152. Plaintiff realleges and incorporates by reference all the preceding paragraphs and  
22 allegations of this Complaint as if fully set forth here.

23 153. Article I, section 1 of the California Constitution provides: "All people are by  
24 nature free and independent and have inalienable rights. Among these are enjoying and defending  
25 life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety,  
26 happiness, and privacy." Art. I., Sec. 1, Cal. Const.

27 154. To state a claim for invasion of privacy under the California Constitution, a plaintiff  
28 must establish (1) a legal protected privacy interest; (2) a reasonable expectation of privacy; and

1 (3) and intrusion so serious in nature, scope, and actual or potential impact as to constitute an  
2 egregious breach of the social norms.

3 155. The right to privacy in California's Constitution creates a right of action against  
4 private and government entities.

5 156. LinkedIn has intruded upon Plaintiff's and Class Members' legally protected  
6 privacy interests, including their: (i) interests in precluding the dissemination or misuse of sensitive  
7 and confidential information ("informational privacy"); (ii) interests in making intimate personal  
8 decisions or conducting personal activities without observation, intrusion, or interference  
9 ("autonomy privacy"); (iii) the Electronic Communications Privacy Act as alleged in Count One;  
10 (iv) the Stored Communications Act, as alleged in Count Two; and (v) the LinkedIn Terms of  
11 Service and Privacy Policy.

12 157. The confidential and sensitive information that LinkedIn intercepted, recorded,  
13 transmitted, and disclosed without Plaintiff and Class Members' authorization and/or consent  
14 included, for example, Plaintiff's and Class Members' private text messages, photos, e-mails, and  
15 the contents of the webpages they visited and/or interacted with, including secure webpages.  
16 Plaintiff and Class Members had a legally protected informational privacy interest in this  
17 confidential and sensitive information, as well as an autonomy privacy interest in conducting their  
18 personal activities without observation, intrusion, or interference.

19 158. Plaintiff and Class Members had a reasonable expectation of privacy in the  
20 circumstances alleged in this Complaint in that: (i) LinkedIn's invasion of privacy occurred as  
21 Plaintiff and Class Members placed information into their local device clipboards and/or cross-  
22 device Universal Clipboards for their own personal use; (ii) the information placed in local device  
23 clipboards and the cross-device Universal Clipboard includes highly sensitive information such as  
24 photos, text messages, e-mails, health records, cryptographic keys, and other private information;  
25 and (iii) Plaintiff and Class Members could not reasonably expect LinkedIn would commit acts in  
26 violation of federal and state laws protecting privacy to repeatedly and without consent read and  
27 use the sensitive information from their local device clipboards and cross-device Universal  
28 Clipboards.

1           159. LinkedIn’s actions constituted a serious invasion of privacy that would be highly  
2 offensive to a reasonable person in that: (i) the invasion occurred within a zone of privacy protected  
3 by the California Constitution, namely the collection of unnecessary information by businesses  
4 without consent, and the misuse of information gathered for one person in order to serve other  
5 purposes; (ii) the invasion deprived Plaintiff and Class Members of the ability to control circulation  
6 of personal information, which is considered fundamental to the right of privacy; and (iii) the  
7 invasion violated several federal and state laws, including, among others, the Electronic  
8 Communications Privacy Act and the Stored Communications Act.

9           160. LinkedIn’s invasion violated the privacy rights of Plaintiff—as well as hundreds of  
10 thousands, if not millions, of Class Members—without Plaintiff’s or Class Members’ authorization  
11 or consent. LinkedIn’s illegal acts against hundreds of thousands, if not millions, of its own app  
12 users (including Plaintiff and Class Members), constituted and constitutes an egregious breach of  
13 social norms.

14           161. LinkedIn’s surreptitious and unauthorized interception, capture, and misuse of  
15 hundreds of thousands, if not millions, of LinkedIn App users’ (including Plaintiff’s and Class  
16 Members’) personal confidential information constituted an egregious breach of social norms.

17           162. LinkedIn lacked any compelling or legitimate business interest in intercepting,  
18 capturing, and reading the personal, private, and confidential information of hundreds of  
19 thousands, if not millions, of LinkedIn App users (including Plaintiff and Class Members), who  
20 did not consent or authorize LinkedIn’s behavior. Plaintiff specifically did not consent to,  
21 authorize, or know about the LinkedIn behavior alleged in this Complaint.

22           163. LinkedIn intentionally engages in the misconduct described here to, at minimum,  
23 use information mined from users’ local and cross-device clipboards to increase the monetization  
24 of its mobile products, generating substantial profits.

25           164. As a result of LinkedIn’s actions, Plaintiff and Class Members have been damaged  
26 as a direct and proximate result of LinkedIn’s invasion of privacy and are entitled to just  
27 compensation.  
28



1 As a Visitor or Member of our Services, the collection, use and  
2 sharing of your personal data is subject to this Privacy Policy  
3 [hyperlink] (which includes our Cookie Policy and other documents  
4 referenced in this Privacy Policy) and updates.

5 172. The User Agreement thus incorporates the Privacy Policy by reference. The Privacy  
6 Policy, along with other incorporated documents, are all part of the contract between Plaintiff and  
7 Class Members, and LinkedIn.

8 173. The Privacy Policy states that the following information is collected about a user's  
9 device and location:

10 **1.5 Your Device and Location**

11 When you visit or leave our Services (including some plugins and  
12 our cookies or similar technology on the sites of others), we receive  
13 the URL of both the site you came from and the one you go to and  
14 the time of your visit. We also get information about your network  
15 and device (e.g., IP address, proxy server, operating system, web  
16 browser and add-ons, device identifier and features, cookie IDs  
17 and/or ISP, or your mobile carrier). If you use our Services from a  
18 mobile device, that device will send us data about your location  
19 based on your phone settings. We will ask you to opt-in before we  
20 use GPS or other tools to identify your precise location.

21 174. The Privacy Policy is granular about what information is collected, including on  
22 mobile devices. It does not state that the LinkedIn App reads information from the local device  
23 clipboard or cross-device Universal Clipboard without a user-initiated paste command—or other  
24 authorization or consent to read information from those sources. Indeed, the Privacy Agreement  
25 makes no mention at all of the local device clipboard and/or the cross-device Universal Clipboard.

26 175. Likewise, the Privacy Policy's Section 1.1 explains that information is collected  
27 when a user fills out forms and interacts with LinkedIn, but it omits that information is also  
28 collected from the local device clipboard and/or cross-device Universal Clipboard without  
notification to, or consent from, the user. Indeed, the Privacy Policy says nothing at all about local  
device clipboard and/or cross-device Universal Clipboard information being collected upon  
interaction with text boxes in LinkedIn:

1                   **Posting and Uploading**

2                   We collect personal data from you when you provide, post, or  
3                   upload it to our Services, such as when you fill out a form, (e.g.,  
4                   with demographic data or salary), respond to a survey, or submit a  
5                   resume or fill out a job application on our Services. If you opt to  
6                   import your address book, we receive your contracts (including  
7                   contract information your service provider(s) or app automatically  
8                   added to your address book when you communicated with addresses  
9                   or numbers not already on your list).

10                   If you sync your contacts or calendars with our Services, we will  
11                   collect your address book and calendar meeting information to keep  
12                   growing your network by suggesting connections for you and others,  
13                   and by providing information about events, e.g., times, places,  
14                   attendees and contacts.

15                   *You don't have to post or upload personal data;* though if you  
16                   don't, it may limit your ability to grow and engage with your  
17                   network over our Services.

18 (emphasis added)

19                   176.    The Privacy Policy is clear: information is voluntarily provided, and there is no  
20                   requirement to provide information. Moreover, there is no disclosure that interaction with forms  
21                   on LinkedIn while using the LinkedIn App will result in the reading of the local device clipboard  
22                   and/or cross-device Universal Clipboard without notice to, or consent from, the user.

23                   177.    LinkedIn's statements about its data collection, storage, and use constitute a  
24                   promise that is legally binding and integral and material to its contracts with Plaintiff and Class  
25                   Members. LinkedIn breached its promises about the scope of its data collection and omitted  
26                   material facts in its disclosures about its practices.

27                   178.    LinkedIn, by speaking partially, has a duty to speak fully and truthfully. By failing  
28                   to tell the whole truth about how and when it collects data from users and/or uses data from users,  
29                   it has breached its contract.

30                   179.    As a result of the breaches of the contracts with Plaintiff and Class Members,  
31                   Plaintiff and Class Members have suffered damages in an amount to be determined at trial.  
32                   Specifically, the services Plaintiff and Class Members have received are worth less than the

1 personal information they exchanged for those services. Moreover, LinkedIn is unjustly enriched  
2 and/or must make restitution for profiting from its breach of contract.

3 180. In addition, or in the alternative, Plaintiff and the Class Members seek damages that  
4 will reasonably compensate Plaintiffs and Class Members for the harms to their privacy interest  
5 from LinkedIn's behavior. By obtaining local device clipboard and cross-device Universal  
6 Clipboard information without user consent, LinkedIn invaded Plaintiff's and Class Members'  
7 privacy interests. As a result, Plaintiff and Class Members have suffered damages.

8 181. Indeed, photos, text messages, e-mails, and portions of websites, including secured  
9 websites, are highly valuable to LinkedIn because this information can be mined using machine  
10 learning to make its app and social network more predictive and better suited to serve content and  
11 advertising to users. The precise value and content of what LinkedIn took through the misbehavior  
12 of the LinkedIn App set forth in this Complaint requires information that is likely to be exclusively  
13 in the possession, custody, and control of LinkedIn, and the value of that content will require  
14 discovery of LinkedIn's business practices, including expert discovery. Plaintiff and Members of  
15 the Class routinely copied or cut the sort of highly valuable information described in the first  
16 sentence of this paragraph (photos, text messages, e-mails, portions of websites, etc.) into their  
17 continuity-enabled Apple device clipboards, and LinkedIn has been unjustly enriched by  
18 improperly and without authorization accessing and using this information.

19 182. LinkedIn engages in the conduct alleged in this Complaint to increase the value and  
20 monetizability of its LinkedIn App and LinkedIn social network, and generates substantial profit  
21 as a result. Plaintiff and Class Members are entitled to disgorgement of profits LinkedIn has  
22 obtained as a result of enhanced value from surreptitiously accessing and using information from  
23 local device clipboards and cross-device Universal Clipboards without user consent.

24 **COUNT SIX**  
25 **(on behalf of Plaintiff and the Nationwide LinkedIn App User Class)**  
26 **Violation of the California Unfair Competition Law,**  
27 **Cal. Bus. & Prof. Code § 17200, et seq.**

28 183. Plaintiff realleges and incorporates by reference all the preceding paragraphs and  
allegations of this Complaint as if fully set forth here.



1           184. LinkedIn engaged in business acts and practices deemed “unlawful” under the  
2 UCL, because, as alleged above, LinkedIn unlawfully, intercepted, obtained, acquired, used,  
3 and/or misused Plaintiff’s and Class Members’ local device clipboard and cross-device Universal  
4 Clipboard information, including sensitive information stored therein, without consent in violation  
5 of the Electronic Communications Privacy Act, the Stored Communications Act, California  
6 common law, and the California Constitution.

7           185. LinkedIn also engaged in business acts or practices deemed “unfair” under the UCL  
8 because, as alleged above, LinkedIn failed to disclose during the Class Period that the LinkedIn  
9 App was reading from local device clipboards and cross-device Universal Clipboards without  
10 users’ consent or knowledge.

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

19           187. First, as described above, LinkedIn’s conduct violates the policies of (at least) the  
20 Electronic Communications Privacy Act, the Stored Communications Act, California common  
21 law, and the California Constitution. Second, the gravity of the harm from LinkedIn’s secret  
22 interception, acquisition, capture, and misuse of Plaintiff’s and Class Members’ communications  
23 is significant, and there is no corresponding benefit to consumers from such conduct. Third,  
24 because Plaintiff and Class Members were completely unaware of LinkedIn’s secret acquisition of  
25 local device clipboard and cross-device Universal Clipboard contents, they could not have possibly  
26 avoided the harm.

27           188. Had Plaintiff and Class Members known that their communications would be  
28 intercepted, acquired, captured, and/or misused, they would not have downloaded and used the

1 LinkedIn App and/or would not have used the LinkedIn service. By surreptitiously intercepting,  
2 acquiring, capturing, and/or misusing local device clipboard and cross-device Universal Clipboard  
3 information, LinkedIn has taken property from Plaintiff and Class Members without providing just  
4 or any compensation.

5 189. Plaintiff, individually and on behalf of the Class, seeks an injunction enjoining  
6 LinkedIn from engaging in the unlawful conduct alleged in this Count.

7 **PRAYER FOR RELIEF**

8 WHEREFORE, Plaintiffs pray that this Court:

9 **A.** Enter an order certifying this case as a class action pursuant to Federal Rule of Civil  
10 Procedure 23;

11 **B.** Enter a judgment declaring that Defendant has committed the violations of law  
12 alleged in this case;

13 **C.** Award actual, compensatory, statutory, punitive, and/or consequential damages, as  
14 called for by the respective statutes and other causes of action violated by Defendant;

15 **D.** Award Plaintiff the costs of this action, including reasonable attorneys’ fees and  
16 expenses and expert fees;

17 **E.** Enjoin Defendant from continue to improperly access information, including  
18 electronic communications, stored on iOS and MacOS clipboards and/or the Universal Clipboard.

19 **F.** Award declaratory relief;

20 **G.** Award pre-judgment and post-judgment interest at the highest rate allowed by law;  
21 and

22 **H.** Grant such further relief as this Court may deem just and proper.  
23  
24  
25  
26  
27  
28

**JURY DEMAND**

Pursuant to Federal Rule of Civil Procedure 38, Plaintiffs, individually and on behalf of the Class they seek to represent, demand a jury on any issue so triable of right by a jury.

Dated: July 10, 2020

Respectfully submitted,

/s/ Brian J. Dunne  
Brian J. Dunne (CA 275689)  
bdunne@bathaeedunne.com  
**BATHAEE DUNNE LLP**  
633 West Fifth Street, 26th Floor  
Los Angeles, CA 90071  
Tel: (213) 462-2772

Yavar Bathaee (CA 282388)  
yavar@bathaeedunne.com  
Edward M. Grauman\* (NY 4196390)  
egrauman@bathaeedunne.com  
Andrew C. Wolinsky\* (NY 4892196)  
awolinsky@bathaeedunne.com  
**BATHAEE DUNNE LLP**  
445 Park Avenue, 9th Floor  
New York, NY 10022  
Tel: 332 205-7668

*Attorneys for Plaintiffs*

---

\* *Pro hac vice* to be sought.