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

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

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

Plaintiffs,

vs.

LinkedIn Corporation,

Defendant.

Case Number: _____

Class Action Complaint
Jury Trial Demanded

* *Pro hac vice* to be sought.

TABLE OF CONTENTS

INTRODUCTION

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

* * *

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

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

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

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

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

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

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

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

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

11. This action seeks to hold LinkedIn responsible for its misbehavior.

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 form 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.

20. Plaintiff routinely uses (and during the Class Period used) the LinkedIn App while also storing information such as the information identified in the previous paragraph in his device clipboards, including on the clipboards of nearby devices while using the LinkedIn App.

21. Plaintiff did not expect that information in the clipboards of his devices, including nearby devices, would be read by LinkedIn unless he entered a "paste" command on his device. He was not aware that apps or any other software had access to this information without his affirmative consent by means of a paste command.

22. If Plaintiff knew the truth about LinkedIn's surreptitious reading of the contents of his clipboards, including the Universal Clipboard populated by nearby devices, he would not have used the LinkedIn App.

JURISDICTION AND VENUE

23. This Court has subject matter over the claims in this action under 28 U.S.C. § 1331 because all claims arise under federal law. This Court may exercise supplemental jurisdiction pursuant to 28 U.S.C. § 1367 over the remaining state common law and statutory claims as these state law claims are part of the same case or controversy as the federal statutory claims over which the Court has original jurisdiction.

24. This Court also has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action, including claims asserted on behalf of a nationwide class, filed under Rule 23 of the Federal Rules of Civil Procedure; there are likely to be hundreds of thousands if not millions of putative class members; and the amount in controversy exceeds the jurisdictional amount of $5 million.

25. This Court has personal jurisdiction over LinkedIn because its headquarters is based in California, because it conducts substantial business from which the claims in this case arise in California, and because LinkedIn has agreed to personal jurisdiction in this Court.

26. Venue is appropriate in this judicial district pursuant to 28 U.S.C. § 1391 because LinkedIn is headquartered in this judicial district and because LinkedIn has agreed that venue is proper in this district.

FACTS

III. THE APPLE UNIVERSAL CLIPBOARD

A. Apple's Handoff Feature

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

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

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

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

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

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

32. Handoff requires that Apple's "continuity" conditions be met, which include that: (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

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

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

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

B. The Universal Clipboard

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

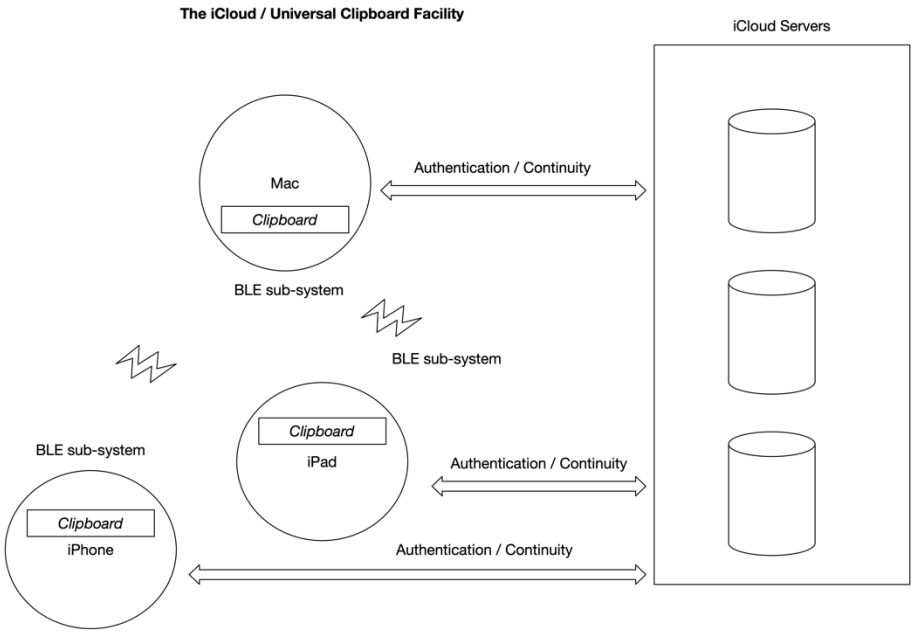
36. Information is "cut" or "copied" to a clipboard, and then "pasted" in another location. If information is "cut" from a location, it is removed from that location and placed in the clipboard. If it is copied, it remains in the original location and a copy is placed on the clipboard. Information on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

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

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

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

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



41. This facility's purpose is to provide electronic communications across devices, including by communicating with Apple's iCloud, an electronic communications service that electronically stores and maintains electronic information for iCloud users across various Apple devices.

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

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

44. As Apple explains on its support page:

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

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

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

> - Copy on a device: Select the content you want to copy, then copy it. For example, on your Mac, press Command-C or choose Edit > Copy.
>
> The copied content is available to paste on your other devices only for a short time.
>
> - Paste on a device: Position the pointer where you want to paste the content, then paste it. For example, on your iPad, double tap, then choose Paste from the options.

47. The Universal Clipboard operates both as a conventional clipboard, allowing copy, 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

> **Copy, cut, or paste**
>
> - Copy: Pinch closed with three fingers.
> - Cut: Pinch closed with three fingers two times.
> - Paste: Pinch open with three fingers.
>
> You can also touch and hold a selection, then tap Cut, Copy, or Paste.

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

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

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

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

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

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

V. LINKEDIN'S IOS APP REPEATEDLY READS THE CONTENTS OF THE UNIVERSAL CLIPBOARD WITHOUT USER PERMISSION.

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

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

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

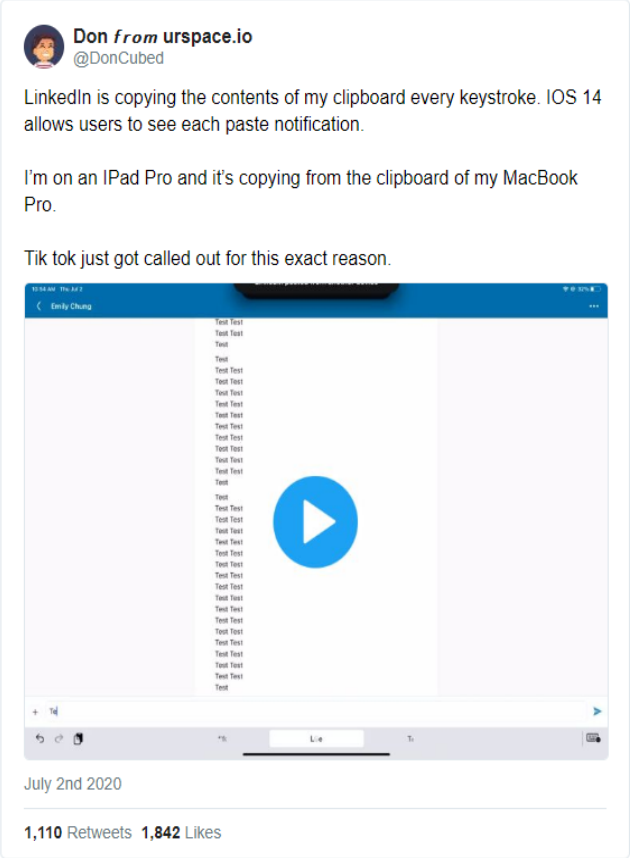
71. The LinkedIn App is developed by LinkedIn and distributed on Apple's App Store for iOS devices, including the iPhone and iPad, which are some of the most popular mobile and touch-enabled devices in the United States.

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

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

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

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



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

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

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

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

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

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

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

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

83. Because the data transferred through the Universal Clipboard expires on remote devices after 120 seconds, the LinkedIn App is designed to circumvent the timer by reading the 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

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

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

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

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

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

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

89. Moreover, LinkedIn never disclosed in any user agreement or public website that it reads the contents of user clipboards, including electronic communications cut or copied to the 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.

Numerosity and Ascertainability

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

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

Predominance of Common Issues

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

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

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

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

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

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

f. Whether LinkedIn's conduct was unlawful.

Typicality

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

Adequate Representation

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

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

Superiority

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

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

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

103. The conduct of this action as a class action presents far fewer management difficulties, far better conserves judicial resources and the parties' resources, and far more effectively protects the rights of each Class member than would piecemeal litigation. Compared to the expense, burdens, inconsistencies, economic infeasibility, and inefficiencies of individualized litigation, the challenges of managing this action as a class are substantially outweighed by the benefits to the legitimate interests of the parties, the court, and the public of class treatment in this Court, making class adjudication superior to other alternatives, under Fed. R. Civ. P. 23(b)(3)(D).

104. Plaintiffs are not aware of any obstacles likely to be encountered in the management of this action that would preclude its maintenance as a class action. Rule 23 provides the Court with authority and flexibility to maximize the efficiencies and benefits of the class mechanism and reduce management challenges. The Court may, on motion of Plaintiffs or on its own determination, certify nationwide, statewide, and/or multistate classes for claims sharing common legal questions; utilize the provisions of Rule 23(c)(4) to certify any particular claims, issues, or common questions of fact or law for class-wide adjudication; certify and adjudicate bellwether class claims; and utilize Rule 23(c)(5) to divide any class into subclasses.

CLAIMS FOR RELIEF

COUNT ONE
(on behalf of Plaintiff and the Continuity Class)
THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
(18 U.S.C. § 2510, *et seq.*)

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

106. LinkedIn designs, develops, releases, and supports interactive software applications for Apple iOS devices, including the LinkedIn native app for Apple iPhone and Apple iPad (the "LinkedIn App").

107. LinkedIn, through the LinkedIn App, surreptitiously abuses Apple's Universal Clipboard, in violation of 18 U.S.C. § 2510, *et seq.*

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

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

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

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

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

- When a person is using the LinkedIn App on their iPhone or iPad (here, the "LinkedIn iOS Device") and a copy command is entered on a nearby continuity-enabled Apple device (*e.g.*, a Macintosh computer, iPhone, or iPad signed into the same Apple ID), the information copied on the continuity-enabled Apple device is pushed via a Continuity Subsystem to temporary storage on the LinkedIn iOS Device. Without the user's knowledge or approval, the LinkedIn App intercepts the pushed information through a surreptitious clipboard read upon the first 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). Upon the LinkedIn App's intercept of the pushed information from the separate continuity-enabled Apple device, the 120-second timer limiting the persistence of that information on the LinkedIn iOS Device is destroyed without the user's knowledge or consent. Thereafter, the LinkedIn App—and any other applications on the LinkedIn iOS App that may later be used before a new item is copied to the clipboard—may use, disclose, or otherwise access the intercepted information at their leisure, ***without the LinkedIn App user ever realizing that information copied on a different Apple device has covertly been intercepted and redirected to a persistent, local clipboard on the LinkedIn iOS Device.***

[1] Plaintiff has reason to believe, but has not yet confirmed, that LinkedIn also violates 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

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

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

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

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

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

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

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

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

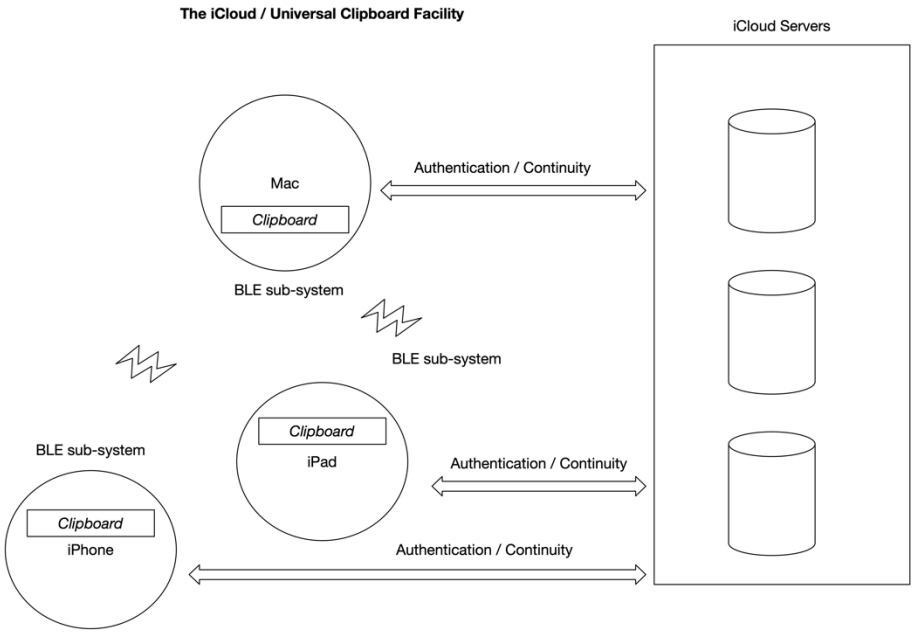
COUNT TWO
(on behalf of Plaintiff and the Continuity Class)
THE STORED COMMUNICATIONS ACT
(18 U.S.C. § 2701, *et seq*.)

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

165. Plaintiff and Class Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests, as well as disgorgement of profits made by LinkedIn as a result of its invasion of Plaintiff and Class Members' privacy.

COUNT FIVE
(on behalf of Plaintiff and the Nationwide LinkedIn App User Class)
Breach of Contract

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

167. As detailed below, Plaintiff entered into a valid contract with LinkedIn, a contract which LinkedIn breached by intercepting, reading, and making use of information in Plaintiff's and Class Members' local device clipboard and cross-device Universal Clipboard without their consent.

168. Plaintiff and Class Members downloaded the LinkedIn App from the Apple App Store. In order to use the LinkedIn app, Plaintiff and Class Members must create or already possess a LinkedIn account and agree to LinkedIn's User Agreement and the LinkedIn Privacy Policy.

169. By agreeing to the LinkedIn User Agreement and Privacy Policy, Plaintiff and Class Members have fully complied with their obligations under those agreements with regard to their use of LinkedIn's services.

170. The User Agreement purports to be a legally binding contract. It states:

> You agree that by clicking "Join Now", "Join LinkedIn", Sign Up" or similar, registering, accessing or using our services (described below), you are agreeing to enter into a legal binding contract with LinkedIn (even if you are using our Services on behalf of a company). If you do not agree to this contract ("Contract" or "User Agreement"), do **not** click "Join Now" (or similar) and do not access or otherwise use any of our Services. If you wish to terminate this contract, at any time you can do so by closing your account and no longer accessing or using our Services.

(emphasis in the original).

171. The User Agreement incorporates by reference the LinkedIn Privacy Policy. The User Agreement states:

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

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

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

> **1.5 Your Device and Location**
>
> When you visit or leave our Services (including some plugins and our cookies or similar technology on the sites of others), we receive the URL of both the site you came from and the one you go to and the time of your visit. We also get information about your network and device (*e.g.*, IP address, proxy server, operating system, web browser and add-ons, device identifier and features, cookie IDs and/or ISP, or your mobile carrier). If you use our Services from a mobile device, that device will send us data about your location based on your phone settings. We will ask you to opt-in before we use GPS or other tools to identify your precise location.

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

175. Likewise, the Privacy Policy's Section 1.1 explains that information is collected when a user fills out forms and interacts with LinkedIn, but it omits that information is also 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:

> **Posting and Uploading**
>
> We collect personal data from you when you provide, post, or upload it to our Services, such as when you fill out a form, (*e.g.*, with demographic data or salary), respond to a survey, or submit a resume or fill out a job application on our Services. If you opt to import your address book, we receive your contracts (including contract information your service provider(s) or app automatically added to your address book when you communicated with addresses or numbers not already on your list).
>
> If you sync your contacts or calendars with our Services, we will collect your address book and calendar meeting information to keep growing your network by suggesting connections for you and others, and by providing information about events, *e.g.*, times, places, attendees and contacts.
>
> ***You don't have to post or upload personal data***; though if you don't, it may limit your ability to grow and engage with your network over our Services.

(emphasis added)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray that this Court:

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

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

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

D. Award Plaintiff the costs of this action, including reasonable attorneys' fees and expenses and expert fees;

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

F. Award declaratory relief;

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

H. Grant such further relief as this Court may deem just and proper.

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.