Stephen R. Basser
E-mail: sbasser@barrack.com
Samuel M. Ward
E-mail: sward@barrack.com
BARRACK RODOS & BACINE
One America Plaza
600 West Broadway, Suite 900
San Diego, CA 92101
Telephone: (619) 230-0800
Facsimile: (619) 230-1874

Attorneys for Plaintiff Nathan Dluzak

Additional Counsel listed on Signature Page

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

NATHAN DLUZAK, individually and on behalf of all others similarly situated, Plaintiff v. APPLE, INC., Defendant	Case No. _____ CLASS ACTION COMPLAINT **JURY TRIAL DEMANDED**

Plaintiff Nathan Dluzak, individually and on behalf of all others similarly situated ("Plaintiff"), brings this class action complaint against Apple, Inc. ("Apple" or "Defendant"), and alleges, upon personal knowledge as to his own actions, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. This case is a proposed class action brought against Apple arising from its long-standing and ongoing invasion of the privacy of consumers who use Apple mobile devices, despite leading such consumers utilizing its mobile devices and related proprietary applications ("Apps") – including the App Store, Apple Music, Apple TV, Books, and Stocks – to believe that their privacy was and is protected once they chose to indicate through the mobile device settings that they do not want their data and information tracked by Apple or consequently shared with third parties.

2. Privacy is an important right and expectation of citizens. Contrary to its express privacy promises, as discussed more fully below, Apple tracks and collects an enormous wealth of data and personal information from its mobile device users while they are using its propriety applications (hereinafter "Mobile Device Consumers"), irrespective of the fact that Mobile Device Consumers – Plaintiff and Class Members herein – have their user privacy settings set so as to intentionally stop or preclude any tracking of their usage and consequent sharing or transmission of their data usage with third parties. Apple aggressively collects, transmits, exploits, and uses for its financial gain, details about Mobile Device Consumers' usage, browsing, communications, personal information, and even information relating to the Mobile Device itself (collectively "User Data"), without the consent or authorization of Mobile Device Consumers.

3. Apple flagrantly engages in such conduct even though it knows that consumers want to keep their User Data private, and expect and demand control over their own such data, out of an increasing concern that companies are using such information without their knowledge or permission, and, worse yet, profiting from such exploitative tracking. Hypocritically, Apple has portrayed and has attempted to distinguish itself from competitors by various representations to its Mobile Device Consumers that they are able to control the information stating: "At Apple,

we respect your ability to know, access, correct, transfer, restrict the processing of, and delete your personal data."

4. Apple further declares through its Apple App Store "User Privacy and Data Use" page that:

> The App Store is designed to be a safe and trusted place for users to discover apps created by talented developers around the world. Apps on the App Store are held to a high standard for **privacy**, **security** and **content** because **nothing is more important than maintaining users trust**. (Emphasis added).

5. Nonetheless, Apple contradicts these and other explicit privacy promises by tracking and collecting large amounts of personal information in violation of Mobile Device Consumers' wishes. Indeed, such Mobile Device Consumers – including Plaintiff and Class Members – are deceived into believing that they have protected themselves by disabling the sharing of their User Data once they toggle or turn off "Share iPad Analytics" on an iPad, "Share iPhone, and Computer Analytics," or similar settings on other Apple mobile devices like the iPhone, or by turning off "Allow Apps to Request to Track," ostensibly disabling Apple from collecting and using User Data without their consent.

6. Plaintiff is an individual whose mobile app usage was tracked by Apple after he had affirmatively elected to turn off the "Allow Apps to Request to Track" and/or "Share [Device] Analytics" options.

7. Apple's tracking and hoarding of the User Data of Plaintiff and all other Class Members, and collecting and monetizing their information without their consent, is a violation of Apple's promises and a violation of the law for which it is liable.

8. Plaintiff brings this action individually and on behalf of a class of all citizens nationwide, and all citizens of the State of Illinois, whose User Data was tracked and collected by Apple, without their consent, and seeks all civil remedies provided under the causes of action, including but not limited to compensatory, statutory and/or punitive damages, and attorney's fees and costs.

II. JURISDICTION AND VENUE

9. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant. This court also has federal subject matter jurisdiction under 28 U.S.C. § 1331 with respect to claims for the violation of Federal law and statutes, including but not limited to the Electronic Communications Act ("ECPA"), 18 U.S.C. § 2510, *et seq.*

10. The Northern District of California has personal jurisdiction over the Defendant named in this action because Defendant's headquarters is located within the District and Defendant conducts substantial business in the District through its headquarters, offices, and/or affiliates.

11. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District.

III. THE PARTIES

Plaintiff

12. Plaintiff Nathan Dluzak ("Dluzak" or "Plaintiff") is a resident of New Lenox, Illinois. He owns an Apple iPhone 13 with iOS version 16.1 installed, and has previously owned an iPhone 10XR that he purchased in approximately 2019 or 2020. Plaintiff Dluzak regularly accesses Apple Apps including the App Store, Apple Music, Maps, and Weather. Plaintiff does not wish to be tracked regarding his usage of Apple Mobile Devices and apps, and, to that end, after purchasing his iPhone devices and with respect to his settings, turned off the "Allow Apps to Request to Track" and declined the "Share iPhone Analytics" options. Nevertheless, Apple has both tracked and accessed his User Data despite the fact that Plaintiff had not consented to or otherwise authorized said tracking as Plaintiff has thereafter received targeted advertisements specific to his habits in using his iPhone.

Defendant

13. Defendant Apple, Inc., is incorporated in California and maintains its principal place of business at One Apple Park Way, Cupertino, CA 95014.

IV. FACTUAL ALLEGATIONS

A. Apple Mobile Device Consumers Reasonably Expect Privacy When Using Their Mobile Devices

14. Apple, with sales of over $378 billion in 2022 and a market capitalization of approximately $2.28 trillion, has been and remains the world's largest technology company. It produces highly popular mobile electronic devices, including the iPhone and the iPad.

15. The iPhone – Apple's most valuable product – leads the smartphone market worldwide with a market share of over 28%, and more than 1.2 billion iPhone users throughout the world – it is a singular product that has been credited with vaulting Apple into the position of one of the world's most valuable enterprises. Apple also produces the iPad, a tablet computer device that has sold more than 500 million iPads, and is one of the world's most popular tablet computer devices. In the third quarter of 2022 alone, Apple sold 142 million iPads, claiming 38% of that market.

16. Apple's iPhone and iPad come loaded with Apple's proprietary applications, including the App Store, Apple Music, Apple TV, Books, and Stocks.

17. Mobile Device Consumers reasonably expect their activity will not be shared without affirmative consent. Individual freedom from unauthorized or unwarranted intrusion into one's privacy is highly valued in California, where Apple is incorporated and headquartered, and across America. To many, including Plaintiff, it is a sacred right. Reflecting its importance, California has adopted privacy laws that prohibit and render unlawful unauthorized recording of confidential communications. These laws apply to Apple, a California corporation, and protect all victims, including Plaintiff and Mobile Device Consumers.

18. The right of privacy afforded by 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**." (Emphasis added).

19. The phrase "and privacy" was added in 1972. The legislative intent in doing so was to curb businesses' control over the unauthorized collection and use of consumers' personal information. The legislative record states:

> The right of privacy is the right to be left alone…It prevents government and business interests from **collecting** and **stockpiling** unnecessary **information** about us and from **misusing information gathered** for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulation of **personal information**. This is essential to social relationships and personal freedom.[1]

(Emphasis added).

20. Various studies regarding the collection of consumers' personal data confirm that the surreptitious taking of User Data, personal, confidential, and private information violates expectations of privacy that have been established as general social norms. An overwhelming majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares personal data. A Consumer Reports study found that 92% of Americans believe that internet companies should be required to obtain consent before selling or sharing their data, and the same percentage of Americans believe internet companies should be required to provide consumers with a complete list of the information that has been collected about them.[2] But Apple's conduct is far worse given that its Mobile Device Consumers explicitly tell Apple that they **do not want their communications monitored**, despite which Apple goes ahead and does so, ignoring their explicit wishes.

21. Apple's tracking and data collection respecting Plaintiff, and Class Members has included detailed data collected by Apple, whereby Apple created and monetized User Data and enabled interception by third parties without those users' consent.

---

[1] Ballot Pamphlet, Proposed Stats. & Amends. To Cal. Const. With Arguments To Voters, Gen. Election *26 (Nov. 7, 1972) (emphasis added).

[2] Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds, CONSUMER REPORTS (May 11, 2017), https://www.consumerreports.org/consumerreports/consumers-less-confident-about-healthcaredata-privacy-and-car-safety/.

22. A February 25, 2022 article in the Harvard Business Review cites to Industry observers introducing the concept of "surveillance capitalism," referring to "consumers' increasing awareness that their data is bought, sold, and used without their consent—and their growing reluctance to put up with it." Consumer data is highly valuable to businesses. And Apple's Mobile Device Consumers – including Plaintiff and Class Members herein – want to be protected from businesses obtaining their User Data.[3]

B. Apple's Privacy Representations to its Mobile Device Consumers

23. No doubt mindful of the privacy concerns of Mobile Device Consumers, Apple has strived publicly to distinguish itself from competitors as the protector of their privacy.

24. To that end, in 2015, Apple's Chief Executive Officer, Tim Cook, publicly professed Apple's commitment to consumer privacy stating: "We see that privacy is a fundamental human right that people have. We are going to do everything that we can to help maintain that trust ...."[4]

25. No doubt cognizant of privacy concerns, when Apple announced an operating system update in 2021 (*i.e.*, iOS and iPadOS 15.2), it introduced App Tracking Transparency, purportedly requiring all app developers to secure users affirmative consent before tracking their activity through third-party apps and websites.

26. In an April 2021, when describing its privacy practices for iPads and iPhones, including its App Tracking Transparency framework, Apple acknowledged that "privacy is a fundamental human right" and in order to comfort user consumers listed Apple's privacy principles, including "Making sure that users know what data is shared and how it issued, and

[3] Hossein Rahnama & Alex "Sandy" Pentland, The New Rules of Data Privacy, Harvard Business Review (Feb. 25, 2022), https://hbr.org/2022/02/the-new-rules-ofdata-privacy

[4] *Apple CEO Tim Cook: 'Privacy Is A Fundamental Human Right'*, NPR (Oct. 1, 2015), https://www.npr.org/sections/alltechconsidered/2015/10/01/445026470/apple-ceo-tim-cook•privacy-is-a-fundamental-human-right.

that they can exercise control over it":[5] Apple also launched a world-wide ad campaign, featuring an iPhone with the simple yet unequivocal slogan, "Privacy. That's iPhone."[6]

27. In 2022, Mr. Cook re-emphasized Apple's professed and represented commitment to consumer privacy, exclaiming that "Privacy is a fundamental right and we build it into all products and services at Apple. You should be in control of your data--not the highest bidder" in conjunction with a short video that ends with a message "It's your data. iPhone helps keep it that way" and states "Privacy. That's iPhone."[7]

28. Billboards also represented and promised Apple's professed commitment to privacy exclaiming, "What happens on your iPhone, stays on your iPhone," "Your iPhone knows a lot about you. But we don't," an Apple video advertisement touting its privacy campaign, displays a text on the screen stating, "It's your data. iPhone helps keep it that way." And yet in another Apple advertisement, the narrator proclaims, "Your information is for sale. You have become the product," after which, upon introducing Apple's privacy options, the narrator adds, "Whatever you choose is up to you… App Tracking Transparency. A simple new feature that puts your data back in your control."

29. Ostensibly consistent with the concern respecting privacy, Apple purports to offer its Mobile Device Consumers the option to control what App browsing activity data Apple and third party app developers intercept or collect by simply adjusting their device's privacy settings: "App Tracking Transparency" is offered which ostensibly allows device users "to choose whether an app can track your activity across other companies' Apps and websites for the purposes of advertising or sharing with data brokers.[8] "By turning off "Allow Apps to Request

---

[5] https://www.apple.com/privacy/docs/A_Day_in_the_Life_of_Your_Data.pdf

[6] Apple and Privacy, Apple Insider, https://appleinsider.com/inside/apple-and-privacy.

[7] Mehak Agarwal, *'You should be in control of your data', says Apple CEO Tim Cook on privacy*, Business Today (May 19, 2022), https://www.businesstoday.in/technology/news/story/you should-be-in-control-of-your-data-says-apple-ceo-tim-cook-on-privacy-3 34194-2022-05-19.

[8] *If an app asks to track your activity*, Apple (May 10, 2022), https://support.apple.com/enus/HT212025.

to Track" in their device settings, Apple purportedly assures its user consumers that apps "can't access the system advertising identifier (IDFA), which is often used to track" and are "not permitted to track your activity using other information that identifies you or your device, like your email address."[9] Indeed, Apple's "Share iPhone Analytics," "Share iPhone & Watch Analytics," and "Share iPad Analytics," (collective "Share [Device] Analytics") privacy settings make an explicit promise to "disable the sharing of Device Analytics altogether" when switched off.[10] And when a consumer has an Apple Watch connected to their iPhone, it is necessary instead to turn off the setting for "Share iPhone and Watch analytics" in order to avoid and disable tracking of or interception of information or usage. Hereinafter, this setting, across all such devices, is referred to as "Share [Device] Analytics."

30. Apple's explicit representations are intended to create and consequently do create the reasonable impression among consumer users that Apple shall cease collecting, recording, or allowing third parties to intercept all of consumers' app information, usage, or activity once "Allow Apps to Request to Track" and/or "Share [Device] Analytics" settings are turned off. However, Apple knows that such assurances and promises regarding consumer user privacy and disabling or termination of such tracking and interception are false and misleading.

31. However, any reasonable Mobile Device Consumer, after reading Apple's privacy settings, would reasonably believe that by turning off "Share [Device] Analytics" and/or "Allow Apps to Request to Track," Apple does not and would not track User Data. They have been misled.

C. Apple's Mobile Device Consumers' User Data is Surreptitiously Tracked, Collected, Intercepted, and Exploited

32. Apple has, at all times material to the Class Period, continuously represented that its Mobile Device Consumers can prevent Apple from tracking their user app viewing history and

---

[9] *Id.*

[10] *Device Analytics & Privacy*, Apple https://www.apple.com/legal/privacy/data/en/device-analytics/.

activity data by simply turning off "Allow Apps to Request to Track" and/or "Share [Device] Analytics" from their Apple device's privacy controls, including in the precise location where users enable or disable these very settings.

33. In truth, unbeknownst to Plaintiff and Class Members at all times material to their usage, Apple records, tracks, collects, and monetizes analytics data—including browsing history and activity information—regardless of what safeguards or "privacy settings" consumers undertake to protect their privacy. Apple continues to record consumers' app usage, app browsing communications, and personal information in its proprietary Apple Apps, including the App Store, Apple Music, Apple TV, Books, and Stocks even when and despite the fact that consumers follow Apple's own instructions and turn off "Allow Apps to Request to Track" and/or "Share [Device] Analytics" on their privacy controls. And Apple facilitates the transmission to, or interception by, third parties of consumer users' information and usage, which third parties then exploit for pecuniary gain. At no time did Apple disclose that it would continue to track and record user data, even if these steps were performed. Nor Apple did disclose that it could and would collect, aggregate, and analyze user data so that it continued to track individual consumers, even when the Mobile Device Consumers followed Apple's instructions on how to use mobile apps privately to avoid or ostensibly disable any such tracking.

34. Apple's surreptitious tracking, gathering, transmission, and interception of information was and remains in direct contradiction of Apple's privacy promises. Apple Mobile Device Consumers were, in effect, continuing to be spied upon, all the while, without their consent. And Apple knew it.

35. Plaintiff is informed and believes and thereupon alleges that two app developers and security researchers at the software company Mysk recently determined that Mobile Device Consumers' privacy settings did not stop Apple's data collection activity when using a number of Apple apps such as the App Store, Apple Music, Apple TV, Books, and Stocks. (hereinafter the "Mysk Study") Apple's tracking remained constant, even if the privacy settings were turned off. As an example, App Store harvests information about every single thing Mobile Device Consumers do in real time in the app, and collects details about a user's mobile device as well,

including ID numbers, what kind of device was used, the device's screen resolution, the device's keyboard language, and how the user was connected to the internet. The Mysk Study revealed that the Stocks App collected a Mobile Device User's list of watched stocks, the names of stocks viewed and searched for and time stamps when that occurred, as well as news articles a Mobile Device User saw in the Stocks app. The Mysk Study also discovered that, in addition to tracking and collecting wide swaths of User Data from device users who interact with Apple apps, Apple collects a "Directory Services Identifier" that is tied to a mobile device user's iCloud account, linking their name, email address, and more to the harvested User Data.[11] "This data can be sensitive, especially when you consider that merely searching for apps related to topics such as religion, LGBTQ issues, health and addiction can reveal considerable insights and details about a person's life."[12]

36. Apple's Apps function as an electronic or other analogous device that track and collects the content of electronic computer-to-computer communications between Mobile Device Consumers' and the computer servers and hardware utilized by Apple to operate its apps. As such, Apple's tracking and collection of detailed information about Mobile Device Consumers while they use Apple Apps, is in contradiction of its own privacy promises; and the tracked and collected User Data is directly linked to a Mobile Device Consumer.[13]

37. Alternatively, even if the Apps themselves were not a device, the Apps' software is designed to alter the operation of a mobile device by instructing the hardware components of that physical device to run the processes that ultimately intercept the Mobile Device Consumer's communications and transmit them to Apple without the Mobile Device User's knowledge.

---

[11] Mitchel Clark, *iOS developers say Apple's App Store analytics aren't anonymous,* The Verge (Nov. 21, 2022), https://www.theverge.com/2022/11/21/23471827/apple-app-store-data collection-analytics-personal-info-privacy.

[12] Thomas Germain, *Apple Sued for Allegedly Deceiving users With Privacy Settings After Gizmodo Story*, Gizmodo (Nov. 11, 2022), https://gizmodo.com/apple-iphone-privacy-analytics-class-action-suit-1849774313.

[13] *Id.*

38. The User Data intentionally tracked and collected by Apple constitutes "**content**" generated through Plaintiff's and Class Members' use, interaction, and communication with Apple's Apps relating to the substance and/or meaning of Plaintiff's and Class Members' communications with the Apps. Such information is not merely record information regarding the characteristics of the message that is generated in the course of the communication. The mere fact that Apple values, tracks, collects, and transmits this content, confirms that such communications constitute **"content"** that convey substance and meaning to Apple.

D. Apple Mobile Device Consumers' User and Usage Data is Highly Valuable "Currency"

39. The user-consumer information Apple tracks has massive economic value. This is well understood in the e-commerce industry. Personal information is seen as a form of "currency." As Professor Paul M. Schwartz noted in the Harvard Law Review:

> Personal information is an important **currency** in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.

(Emphasis added)

Paul M. Schwartz, Property, Privacy and Personal Data, 117 HARV. L. REV. 2055, 2056– 57 (2004).

40. Website User and usage data – including personal data (*i.e.*, gender, web browser cookies, IP addresses, and device IDs), engagement data and information (*i.e.*, how consumers interact with a business's website, applications, and emails), behavioral data (*i.e.*, customers' purchase histories and product usage information), and attitudinal data (*i.e.*, data on consumer satisfaction) constitutes highly valuable information about consumers that companies use to improve customer experiences, refine their marketing strategies, capture data to sell it, and even secure more sensitive consumer data.

41. By capturing and using customer data reflecting consumer behavior, companies can shape the buying experience and thereby improve their profits. According to reported

research, organizations that "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[14]

42. Advertisers or Sellers pay for ads on a Social Media Platforms ("SMP") like Google or Facebook for each ad shown to a user (per "impression"). Sellers will pay SMPs more for impressions for users they have reason to believe are likely to buy. SMPs sell impressions that can be categorized by keywords of interests and demographics of users, so called "targeted" ads. SMPs use an auction like system called the "Vickrey-Clarke-Groves procedure" ("VCG Bidding"). Sellers bid on the actual user "clicks" of various demographics, and SMPs sell to the higher bidder.

43. It is in the best interests of the bidders to bid highly for ads that are placed strategically to reach people who are likely to buy the product they sell. Hence, VCG bidding encourages targeted advertising. As Facebook collects data, it determines which ads consumers are more likely to click on, thus increasing the value of those ads for advertisers. It then sells them grouped by the number of clicks.[15]

44. A study by the Economics Department at the University of Copenhagen gave an example: "An example of a keyword is 'andelsvurderinger'[16] in the Danish market of Facebook. The average cost per click is 7,56 DKK. This can specify any add for exactly this query and advertise to potential value customers due to the interest." [17]

---

[14] Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, Capturing value from your customer data, McKinsey (Mar. 15, 2017), https://www.mckinsey.com/capabilities/quantumblack/our-insights/capturing-value-from-your-customer-data (last visited on January 30, 2023).

[15] *Selling Keywords, Targeted Advertising, and The Social Dilemma*: *Networks Course blog for INFO 2040/CS 2850/Econ 2040/SOC 2090*. (2022, November 1), https://blogs.cornell.edu/info2040/2022/11/01/selling-keywords-targeted-advertising-and-the-social-dilemma/ (last visited on January 30, 2023).

[16] Danish for "cooperative assessments."

[17] Leo-Hansen, A. (2020, June). How is the VCG mechanism profiting Facebook? Retrieved January 25, 2023, from University of Copenhagen, Faculty of Social Sciences, Department of Economics,

45. The practice has collectively netted fortunes. For example, Facebook heavily relies on it: "Our advertising revenue is dependent on targeting and measurement tools that incorporate data signals from user activity on websites and services that we do not control, and changes to the regulatory environment, third-party mobile operating systems and browsers, and our own products have impacted, and we expect will continue to impact, the availability of such signals, which will adversely affect our advertising revenue."[18] Meta, the parent company of Facebook, reported advertising revenue of $69.66 billion for 2019 alone, up 27% year-over-year.[19] Not surprisingly, Apple's ads contribute billions to its bottom line.[20]

TOLLING

46. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiff did not know (and had no way of knowing) that his User Data and personal information therein was being tracked, intercepted, disclosed, or exploited by Apple or via Apple by third parties because Apple kept this information secret despite the fact that Plaintiff and Class Members had turned off their tracking setting in order to secure their privacy. Apple's failure to abide by its promise and agreement not to track Plaintiff and Class Members was hidden and not made known prior to November 20, 2022 when the Mysk Report revealed it publicly.

CLASS ALLEGATIONS

47. Plaintiff brings this class action on behalf of himself and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, as more fully alleged below.

---

https://www.researchgate.net/publication/345818075_How_is_the_VCG_mechanism_profiting_Facebook (last visited on January 30, 2023).

[18] *SEC filings details.* Meta - Financials - SEC Filings Details. (n.d.), https://investor.fb.com/financials/sec-filings-details/default.aspx?FilingId=13872030 (last visited on January 30, 2023).

[19] *Id.*

[20] Apple, Inc. (n.d.). *Apple, Inc. Form 10-K for the Fiscal Year Ended September 24, 2022.*

48. The Nationwide Class that Plaintiff seeks to represent ("Nationwide Class") is defined as follows:

> **All individuals who, while using an Apple mobile device had their information tracked or intercepted by Apple after turning off or declining "Allow Apps to Request to Track," "Share iPhone Analytics," and/or any other similar setting on an Apple mobile device in order to stop Apple from collecting their mobile app activity.**

49. The Illinois Class that Plaintiff seeks to represent ("Illinois Sub-Class") is defined as follows:

> **All individuals who are residents of Illinois who, while using an Apple mobile device and declining had their information tracked or intercepted by Apple after turning off "Allow Apps to Request to Track," "Share iPhone Analytics," and/or any other similar setting on an Apple mobile device in order to stop Apple from collecting their mobile app activity.**

50. The Nationwide Class and Illinois Class are sometimes also collectively referred to herein as the "Class."

51. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

52. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

53. Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are many tens of thousands and more individuals whose User Data may have been improperly accessed as alleged above, and each Class is apparently identifiable within Defendant's records.

54. Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect Plaintiff's and Class Members' User Data or private information;

b. Whether Defendant had duties not to disclose the Plaintiff's and Class Members' User Data or private information to third parties;

c. Whether Defendant had duties not allow Plaintiff's and Class Members' User Data or private information to be accessed or intercepted by third parties;

d. Whether Defendant had duties not to allow Plaintiff's and Class Members' User Data or private information to be revealed or used for unauthorized purposes;

e. Whether Defendant failed to adequately safeguard Plaintiff's and Class Members' User Data or private information;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their User Data or private information had been or was being tracked, accessed by, provided to, or used by third parties without their consent;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their User Data or private information had been tracked, accessed by, or provided to, third parties without their consent;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' User Data or private information from tracking, interception, transmission, access, or usage.

55. Plaintiff's claims are typical of those of other Class Members because all had their User Data compromised by Apple and/or unauthorized third parties despite electing not to activate features that permitted tracking or sharing and instead, rejecting, disabling, and/or declining such tracking or sharing.

56. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

57. Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

58. Class action litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

59. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources;

the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

60. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

61. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

62. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to safeguard the privacy of their User Data and private information;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to safeguard the privacy of their User Data and private information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to the safeguarding the privacy of or not disclosure User Data and private information;

d. Whether an express or implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that express or implied contract;

e. Whether Defendant breached the express or implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their User Data had been or was being compromised despite their request and agreement that Apple respect their privacy;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to ensure the privacy of User Data and private information and protect Plaintiff's and Class Members' privacy.

COUNT I

Breach of Implied Contract
(On Behalf of Plaintiff, the Nationwide Class, and the Illinois Class)

63. Plaintiff, on behalf of the Nationwide Class, and the Illinois Class re-alleges all of the foregoing allegations as if fully set forth herein.

64. Defendant solicited Plaintiff, the Nationwide Class, and the Illinois Class to purchase iPhones, iPads, and other consumer electronics with visual commercials and print ads, and represented to all such Class Members that, in purchasing Apple products and declining tracking or sharing their User Data, their privacy was maintained and assured.

65. Apple has acknowledged that an invasion of data privacy included the harvesting by others of User Data. Another example defining invasion of data privacy that Apple has acknowledged is not keeping User Data only on the device.

66. In so doing, Plaintiff, the Nationwide Class, and the Illinois Class entered into implied contracts with Apple by which Defendant Apple agreed not to engage in the invasion of user privacy, not to harvest User Data, and to safeguard users from third parties accessing their User Data, including their private information.

67. A meeting of the minds occurred when Plaintiff, the Nationwide Class, and the Illinois Class agreed to, and did, purchase Defendant's products, and declined, rejected, turned off or otherwise disabled tracking or sharing as alleged heretofore in order to protect the privacy of their User Data.

68. Plaintiff, the Nationwide Class, and the Illinois Class fully performed their obligations under the implied contracts with Defendant.

69. By its actions stated within, Defendant breached the implied contracts it made with Plaintiff, the Nationwide Class, and the Illinois Class.

70. Defendant also profited from its surreptitious harvesting of their User Data in addition to invading user privacy.

71. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff, the Nationwide Class, and the Illinois Class have suffered (and will continue to suffer) ongoing, imminent, and unauthorized User Data usage, tracking, and transmission, and loss of the confidentiality of the harvested User Data; and other economic and non-economic harm, from which Defendant and third parties who were given access to such information were unjustly enriched. As a result of Defendant's breach of implied contract, Plaintiff and Class Members are entitled to and demand actual, consequential, and nominal damages.

COUNT II

Invasion of Privacy
(On Behalf of Plaintiff, the Nationwide Class, and the Illinois Class)

72. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above as though fully set forth at length herein.

73. Plaintiff brings this claim individually and on behalf of members of the Nationwide Class and the Illinois Class against Defendant.

74. The right to privacy in California's constitution creates a universal right of action against entities such as Apple.

75. The principal purpose of this constitutional right was to protect against unnecessary information gathering, use, and dissemination by public and private entities, including Apple.

76. To plead a California constitutional privacy claim, a plaintiff must show an invasion of (1) a legally protected privacy interest; (2) where the plaintiff had a reasonable

expectation of privacy in the circumstances; and (3) conduct by the defendant constituting a serious invasion of privacy.

77. As described herein, Apple has intruded upon the following legally protected privacy interests:

a. The California Wiretap Act as alleged herein;

b. A Fourth Amendment right to the privacy of personal data contained on personal computing devices, including web-browsing history, as explained by the United States Supreme Court in the unanimous decision of *Riley v. California*;

c. The California Constitution's guaranteed right to privacy;

d. Apple's Privacy Policy and policies referenced therein, and other public promises it made not to track or record Plaintiff's communications or access their computing devices and apps while "Allow Apps to Request to Track" and/or "Share Device & Watch Analytics" are turned off or otherwise not activated.

78. Plaintiff had a reasonable expectation of privacy under the circumstances in that Plaintiff could not have reasonably expected that Apple would commit acts in violation of civil and criminal laws; and Apple affirmatively promised consumers it would not track or share their communications, or access their computing devices or apps, while they were using an app while in "Allow Apps to Request to Track" and/or "Share [Device] Analytics" were turned off or not activated.

79. Apple's actions constituted a serious invasion of privacy in that it:

a. Invaded a zone of privacy protected by the Fourth Amendment, namely the right to privacy in data contained on personal computing devices, including user data, App activity and App browsing histories;

b. Violated dozens of state criminal laws on wiretapping and invasion of privacy, including the California Invasion of Privacy Act;

c. Invaded the privacy rights of many millions of Americans without their consent;

and

d. Constituted the unauthorized taking of valuable information from many millions of Americans through deceit.

80. Committing criminal acts against many millions of Americans constitutes an egregious breach of social norms that is highly offensive.

81. The surreptitious and unauthorized tracking of the internet communications of millions of Americans, particularly where, as here, they have taken active (and recommended) measures to ensure their privacy, constitutes an egregious breach of social norms that is highly offensive.

82. Apple's intentional intrusion into Plaintiff's internet communications and their computing devices and Apps was highly offensive to a reasonable person in that Apple violated state criminal and civil laws designed to protect individual privacy and against theft.

83. The taking of personally identifiable information from millions of Americans through deceit is highly offensive behavior.

84. Secret monitoring of private App browsing is highly offensive behavior.

85. Wiretapping and surreptitious recording of communications is highly offensive behavior.

86. Apple lacked a legitimate business interest in tracking consumers while use an app while "Allow Apps to Request to Track" and/or "Share [Device] Analytics" were turned off, without their consent.

87. Plaintiff and the Class members have been damaged by Apple's invasion of their privacy and are entitled to just compensation and injunctive relief.

88. Plaintiff and the members of the Class have suffered an injury in fact resulting in the loss of money and/or property as a proximate result of the violations of law and wrongful conduct of Defendant alleged herein, and they lack an adequate remedy at law to address the unfair conduct at issue here. Legal remedies available to Plaintiff and class members are

inadequate because they are not equally prompt and certain and in other ways efficient as equitable relief. Damages are not equally certain as restitution because the standard that governs restitution is different than the standard that governs damages. Hence, the Court may award restitution even if it determines that Plaintiff fails to sufficiently adduce evidence to support an award of damages. Damages and restitution are not the same amount. Unlike damages, restitution is not limited to the amount of money a defendant wrongfully acquired plus the legal rate of interest. Equitable relief, including restitution, entitles the plaintiff to recover all profits from the wrongdoing, even where the original funds taken have grown far greater than the legal rate of interest would recognize. Legal claims for damages are not equally certain as restitution because claims for restitution entail few elements. In short, significant differences in proof and certainty establish that any potential legal claim cannot serve as an adequate remedy at law.

COUNT III

Violation of The California Invasion Of Privacy Act ("CIPA")
California Penal Code § 632
(On Behalf of Plaintiff, the Nationwide Class, and the Illinois Class)

89. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above as though fully set forth herein.

90. Plaintiff brings this claim individually and on behalf of members of the Nationwide Class and Illinois Class against Defendant.

91. The California Invasion of Privacy Act is codified at Cal. Penal Code §§ 630 to 638. The Act begins with its statement of purpose:

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

Cal. Penal Code § 630.

92. Cal. Penal Code § 632(a) provides, in pertinent part:

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

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

94. Apple maintains its principal place of business in California; designed, contrived and effectuated its scheme to track and record consumer communications while they were browsing Apps from their device while "Allow Apps to Request to Track" and/or "Share [Device] Analytics" were turned off; and has adopted California substantive law to govern its relationship with its users.

95. At all relevant times, Apple's tracking and recording of Plaintiff's communications while using an App with "Allow Apps to Request to Track" and/or "Share [Device] Analytics" turned off was without authorization and consent from the Plaintiff.

96. Apple's mobile applications constitute an "amplifying or recording device" under the CIPA.

97. Plaintiff has suffered loss by reason of these violations, including, but not limited to, violation of his rights to privacy and loss of value in their personally identifiable information.

98. Pursuant to California Penal Code § 637.2, Plaintiff has been injured by the violations of California Penal Code § 632, and seeks damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive relief.

COUNT IV

Violation of The Electronic Communications Act ("ECPA"),
18 U.S.C. § 2510, *et seq*.
(On behalf of Plaintiff, the Nationwide Class, and the Illinois Class)

99. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

100. Plaintiff brings this claim individually and on behalf of members of the Nationwide Class and Illinois Class against Defendant.

101. A violation of the ECPA occurs where any person "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any … electronic communication" or "intentionally discloses, or endeavors to disclose, to any person the contents of any … electronic communication, knowing or having reason to know that the information was obtained through the [unlawful] interception of a[n] … electronic communication" or "intentionally uses, or endeavors to use, the contents of any … electronic communication, knowing or having reason to know that the information was obtained through the [unlawful] interception of a[n] … electronic communication." 18 U.S.C. §§2511 (1)(a), (c) – (d).

102. In addition, "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication [ ] while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511 (3)(a).

103. As defined in 18 U.S.C. § 2510 (12), "electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo optical system that affects interstate or foreign commerce."

104. As defined in 18 U.S.C § 2510(4), "intercept" means "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."

105. As defined in 18 U.S.C § 2510(8), "contents" includes "any information relating to the substance, purport, or meaning" of the communication at issue.

106. As defined in 18 U.S.C § 2510(15), an "electronic communication service" means "any service which provides to users thereof the ability to send or receive wire or electronic communications.

107. 18 U.S.C. §2520(a) provides a private right of action to any person whose wire, oral, or electronic communication is intercepted.

108. Plaintiff and the Class members' use of Apple's iPhone and iPad Mobile Devices is an electronic communication under the ECPA.

109. Apple's iPhone and iPad devices – its Mobile Devices used by the Mobile Device Consumers herein – constitute electronic communication service under the ECPA.

110. Whenever Plaintiff and Class members interacted with Apple's Apps, while deploying the no tracking feature, Apple's contemporaneously and intentionally intercepted, and endeavored to intercept Plaintiff's and Class members' electronic communications without their authorization or consent.

111. Whenever Plaintiff and Class members interacted with Apple, through its Apps, after deploying the no tracking feature, Apple tracked, intercepted, and contemporaneously and intentionally disclosed, and endeavored to disclose, the contents of Plaintiff's and Class members' electronic communications to third parties without authorization or consent, knowing or having reason to know that the electronic communications was tracked, intercepted, and obtained in violation of the ECPA.

112. Whenever Plaintiff and Class members interacted with Apple, through Apps, after deploying the no tracking feature, Apple and third parties tracked, intercepted, and contemporaneously and intentionally used, and endeavored to use the contents of Plaintiff's and Class members' electronic communications, for financial purposes without authorization or consent, knowing or having reason to know that the electronic communications were obtained in violation of the ECPA.

113. Whenever Plaintiff and Class members interacted with Apple's Apps after deploying Apple's no tracking features, Apple and third parties contemporaneously and intentionally redirected the contents of Plaintiff's and Class members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication.

114. Whenever Plaintiff and Class members interacted with Apple's Apps after deploying the no tracking feature, Apple contemporaneously and intentionally divulged the contents of Plaintiff's and Class members' electronic communications while those

communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication.

115. Apple and third parties intentionally intercepted and used the contents of Plaintiff's and Class members' electronic communications for the unauthorized purpose of disclosing and, profiting from, Plaintiff's and Class members' communications and User Data.

116. Plaintiff and Class members did not authorize Apple or third parties to acquire the content of their communications for purposes of sharing and selling their identifiable User Data. Defendant is liable for compensatory, exemplary and statutory and consequential damages arising from each such violation.

COUNT V

Violation of Electronic Communications Privacy Act Unauthorized Divulgence by Electronic Communications Service 18 U.S.C. § 2511(3)(a)
(On Behalf of Plaintiff, the Nationwide Class, and the Illinois Class)

117. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

118. The ECPA Wiretap statute provides that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511(3)(a).

119. **Electronic Communication Service**. An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

120. Defendant's Mobile Devices and Apps are electronic communication services. The services provide to users thereof the ability to send or receive electronic communications. In the absence of Defendant's Mobile Devices and Apps, internet users could not send or receive communications regarding Plaintiff's and Class Members' User Data, including their private information.

121. **Intentional Divulgence**. Defendant intentionally designed the Mobile Device App features and was or should have been aware that, if it did not honor a declination of tracking or sharing, it could divulge Plaintiff's and Class Members' User Data.

122. **While in Transmission**. Upon information and belief, Defendant's divulgence of the contents of Plaintiff's and Class Members' User Data communications was contemporaneous with their exchange with Defendant's Mobile Device Apps to which they directed their communications.

123. Defendant divulged the contents of Plaintiff's and Class Members' User Data and related electronic communications without their authorization. Defendant divulged the contents of Plaintiff's and Class Members' User Data and related electronic communications to third parties without Plaintiff's and Class Members' consent and/or authorization.

124. **Exceptions do not apply**. In addition to the exception for communications directly to an ECS or an agent of an ECS, the Wiretap Act states that "[a] person or entity providing electronic communication service to the public may divulge the contents of any such communication as follows:

a. "as otherwise authorized in section 2511(2)(a) or 2517 of this title;"

b. "with the lawful consent of the originator or any addressee or intended recipient of such communication;"

c. "to a person employed or authorized, or whose facilities are used, to forward such communication to its destination;" or

d. "which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency."

18 U.S.C. § 2511(3)(b)

125. Section 2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication

> service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

126. Defendant's divulgence of the contents of Plaintiff's and Class Members' User Data and related electronic communications to third parties was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (1) a necessary incident to the rendition of Defendant's service; nor (2) necessary to the protection of the rights or property of Defendant.

127. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

128. Defendant's divulgence of the contents of User Data and related communications on Defendant's Mobile Devices Apps was not done "with the lawful consent of the originator or any addresses or intended recipient of such communication[s]." As alleged above: (a) Plaintiff and Class Members did not authorize Defendant to divulge the contents of their User Data related communications; and (b) Defendant did not procure the "lawful consent" from Plaintiff and Class Members who were exchanging information.

129. Moreover, Defendant divulged the contents of Plaintiff's and Class Members' communications through individuals who are not "person[s] employed or whose facilities are used to forward such, communication to its destination."

130. The contents of Plaintiff's and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

131. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; punitive damages in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT VI
Violation of
Title II of the Electronic Communications Privacy Act

18 U.S.C. § 2702, *et seq*.
(Stored Communications Act)
(On Behalf of Plaintiff, the Nationwide Class, and the Illinois Class)

132. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

133. Plaintiff brings this claim individually and on behalf of members of the Nationwide Class and Illinois Class against Defendant.

134. The ECPA further provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

135. **Electronic Communication Service.** ECPA defines "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

136. Defendant intentionally procures and embeds various Plaintiff's and Class Members' User Data on its Mobile Devices and related servers and apps, which qualifies as an Electronic Communication Service.

137. **Electronic Storage**. ECPA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

138. Defendant stores the content of Plaintiff's and Class Members' communications on Defendant's Mobile Devices and related apps and servers and files associated with it.

139. When Plaintiff or Class Members make a Mobile Device related app communication and/or submission, the content of that communication is immediately placed into storage.

140. Defendant knowingly divulges the contents of Plaintiff's and Class Members' communications to third parties without authorization.

141. **Exceptions Do Not Apply**. Section 2702(b) of the Stored Communication Act provides that an electronic communication service provider "may divulge the contents of a communication—"

a. "to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient."

b. "as otherwise authorized in Section 2517, 2511(2)(a), or 2703 of this title;"

c. "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;"

d. "to a person employed or authorized or whose facilities are used to forward such communication to its destination;"

e. "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;"

f. "to the National Center for Missing and Exploited Children, in connection with a reported submission thereto under section 2258A."

g. "to law enforcement agency, if the contents (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime;"

h. "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency"; or

i. "to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies Section 2523."

142. Defendant did not divulge the contents of Plaintiff's and Class Members' communications to "addressees," "intended recipients," or "agents" of any such addressees or intended recipients of Plaintiff and Class Members.

143. Section 2517 and 2703 of the ECPA relate to investigations by government officials and have no relevance here.

144. Section 2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary

> incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

145. Defendant's divulgence of the contents of Plaintiff's and Class Members' communications on Defendant's Mobile Device apps to third parties was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (1) a necessary incident to the rendition of the Defendant's services; nor (2) necessary to the protection of the rights or property of Defendant.

146. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

147. Defendant's divulgence of the contents of User Data related information and communications on Defendant's Mobile Device apps was not done "with the lawful consent of the originator or any addresses or intend recipient of such communication[s]." As alleged above: (a) Plaintiff and Class Members did not authorize Defendant to divulge the contents of their communications; and (b) Defendant did not procure the "lawful consent" from Plaintiff or Class members divulge User Data collected from Websites or Apps.

148. Moreover, Defendant divulged or shared the contents of Plaintiff's and Class Members' communications to individuals who are not "person[s] employed or whose facilities are used to forward such, communication to its destination."

149. The contents of Plaintiff's and Class Members' User Data related communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

150. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; punitive damages in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT VII
Violation of The Computer Fraud and Abuse Act (CFAA)
18 U.S.C. § 1030, *et seq*.
(On Behalf of Plaintiff, the Nationwide Class, and the Illinois Class)

151. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

152. Plaintiff's and Class Members' mobile devices are, and at all relevant times have been, used for interstate communication and commerce, and are therefore "protected computers" under 18 U.S.C. § 1030(e)(2)(B).

153. Defendant exceeded, and continues to exceed, authorized access to the Plaintiff's and the Class's protected computers and obtained information thereby, in violation of 18 U.S.C. § 1030(a)(2), (a)(2)(C).

154. Defendant's conduct caused "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I), *inter alia*, because of the secret transmission of Plaintiff's and the Class's private and personally identifiable User Data and content – including the Mobile Device consumers' electronic communications with the device and app, including their mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communications in real-time ("Device Communications") which were never intended for public consumption.

155. Defendant's conduct also constitutes "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV) due to the User Data, including private information of Plaintiff and the Class being made available to Defendant, and/or other third parties without adequate legal privacy protections.

156. Accordingly, Plaintiff and the Class are entitled to "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief."18 U.S.C. § 1030(g).

COUNT VIII

UNJUST ENRICHMENT
(On behalf of Plaintiff, the Nationwide Class, and the Illinois Class)

157. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

158. Defendant benefits from the use of Plaintiff's and Class Members' User Data and private information and unjustly retained those benefits at their expense.

159. Plaintiff and Class Members conferred a benefit upon Defendant in the form of User Data and private information that Defendant tracked and collected from Plaintiff and Class Members and, among other things, also disclosed without their consent to third parties without authorization and proper compensation. Defendant knowingly collected and used this information for pecuniary gain, providing Defendant and third parties with economic, intangible, and other benefits, including substantial monetary compensation.

160. Defendant's conduct damaged Plaintiff and Class Members, all without providing any commensurate compensation to Plaintiff and Class Members.

161. The benefits that Defendant derived from Plaintiff and Class Members were not offered by Plaintiff and Class Members gratuitously and rightly belong to Plaintiff and Class Members. It would be inequitable under unjust enrichment principles in California, Illinois, and every other state for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts, trade practices and deceptive conduct alleged in this Complaint.

162. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the proposed Class, prays for relief and judgment against Defendant as follows:

A. certifying the Class pursuant to Rule 23 of the Federal Rules of Civil Procedure, appointing Plaintiff as representatives of the Class, and designating Plaintiff's counsel as Class Counsel;

B. declaring that Defendant's conduct violates the laws referenced herein;

C. finding in favor of Plaintiff and the Class on all counts asserted herein;

D. awarding Plaintiff and the Class compensatory damages and actual damages, trebled, in an amount exceeding $5,000,000, to be determined by proof;

E. awarding Plaintiff and the Class appropriate relief, including actual, nominal and statutory damages;

F. awarding Plaintiff and the Class punitive damages;

G. awarding Plaintiff and the Class civil penalties;

H. granting Plaintiff and the Class declaratory and equitable relief, including restitution and disgorgement;

I. enjoining Defendant from continuing to engage in the wrongful acts and practices alleged herein;

J. awarding Plaintiff and the Class the costs of prosecuting this action, including expert witness fees;

K. awarding Plaintiff and the Class reasonable attorneys' fees and costs as allowable by law;

L. awarding pre-judgment and post-judgment interest; and

M. granting any other relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: January ___, 2023

/s/ Stephen R. Basser
Stephen R. Basser

BARRACK RODOS & BACINE
Stephen R. Basser
E-mail: sbasser@barrack.com
Samuel M. Ward
E-mail: sward@barrack.com
One America Plaza
600 West Broadway, Suite 900
San Diego, CA 92101
Telephone: (619) 230-0800
Facsimile: (619) 230-1874

John G. Emerson*
jemerson@emersonfirm.com
EMERSON FIRM, PLLC
2500 Wilcrest Drive, Suite 300
Houston, TX 77042
Telephone: (800) 551-8649
Facsimile: (501) 286-4659

Attorneys for Plaintiff and the Putative Nationwide Class and Illinois Class