Michael W. Sobol (CA 194857)
msobol@lchb.com
Nimish R. Desai (CA 244953)
ndesai@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: 415.956.1000
Facsimile: 415.956.1008

Nicholas Diamand
ndiamand@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
250 Hudson Street, 8th Floor
New York, NY 10013-1413
Telephone: 212.355.9500
Facsimile: 212.355.9592

Hank Bates (CA 167688)
hbates@cbplaw.com
jwilliams@cbplaw.com
CARNEY BATES & PULLIAM PLLC
11311 Arcade Drive, Suite 200
Little Rock, AR 72212
Telephone: 501.312.8500

Bradley S. Clanton
brad@clantonlegalgroup.com
CLANTON LEGAL GROUP PLLC
627 Mohawk Avenue
Jackson, MS 39216
Telephone: 601-454-8794
Facsimile: 866-421-9918

Attorneys for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

ANTHONY HENSON and WILLIAM CINTRON,

Plaintiffs,

v.

TURN, INC.,

Defendant.

Case No. 3:15-cv-1497

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

I. INTRODUCTION

1. The private life of Americans has shifted. It used to be that Americans could read a newspaper, listen to the radio, check a box score, watch television, conduct bank transactions, drop the children off at school, go to work, go shopping, or even consult with their doctor, without an anonymous third party tracking and storing all those activities. Practically, only a hired private detective surreptitiously surveilling around the clock would be able to gather all that information.

2. Today, however, because much of Americans' daily routine now takes place online through the use of web browsers or apps, *all* of those activities—and many more—may be monitored and cataloged as a matter of course. To name just some common examples, Americans view news at websites such as www.nytimes.com; listen to radio content through streaming websites like Pandora; use bank websites for managing their finances; shop at online marketplaces like Amazon; use GPS for directions and traffic updates; communicate over email and social network platforms like Facebook; and read sites like WebMD to assess their medical condition. In other words, what used to be mere anecdotes of a person's daily routine shared over coffee or at the water cooler, have become an electronic catalogue of that person's every movement by unknown third parties who transform that information into a marketable product.

3. Increasingly, we use a single device—a smartphone or tablet—to accomplish all of these tasks. Marketing companies, such as Defendant Turn, Inc. ("Turn"), have developed ways to place tracking beacons on these devices—lines of code called "cookies"—through web browsers and other smart phone apps. Cookies monitor and gather information about a user's website browsing and app use which, as noted above, includes personal information regarding one's daily routine. The resulting data is analyzed and used to target advertisements that match the user's profile.

4. Mere use of these online services hardly constitutes consent to the surreptitious tracking and profiling. Online activity is essential to modern life, and there is no way to opt out from it. Turn knows that most people prefer to live their lives in private, and thus do not want their extensive and necessary smartphone activity tracked. A survey Turn conducted with Forbes

magazine found that 54% of consumers felt that their privacy concerns outweighed "*any* benefits derived from sharing information with businesses," and that 56% of consumers "are generally uncomfortable with the amount of information companies know about them or could learn about them through their activities." *The Promise of Privacy: Respecting Consumers' Limits While Realizing the Marketing Benefits of Big Data*, FORBES, at p. 15 (2013), *available at* http://images.forbes.com/forbesinsights/StudyPDFs/turn_promise_of_privacy_report.pdf. (emphasis added).

5. In response to these widespread concerns, manufacturers and software companies developed functions for clearing and blocking cookies, which have long been standard features on all smartphones, tablets, computers, and web browsers. Turn's survey found that 69% of participants deleted cookies in order to "shield their online privacy." *Id*.

6. But rather than respect society's wishes, companies have engaged in what one security expert dubs "a minor arms race," in which the "Internet surveillance industry" has created cookies that evade detection by web users and that cannot be deleted from their machines. Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, 49 (2015).

7. Turn is one such company. For several years, it has secretly exploited a feature of the routing processes of Verizon customers' mobile devices in order to convert those devices into tracking beacons and to monitor the user's behavior. Turn does this in order to harvest data about individuals and build robust data profiles, which it then uses to serve targeted and profitable advertising.

8. Specifically, until its practices were exposed in several media reports in early 2015, Turn utilized a persistent, unique identifier header ("X-UIDH" or "UIDH") that Verizon embeds in the requests to websites that are sent from each customer's mobile device. Each X-UIDH is unique to that customer's device. Turn realized that it could attach that X-UIDH value onto its third-party tracking cookies.

9. As detailed below, by incorporating the X-UIDH into its cookies, Turn was able to store all of the values associated with that X-UIDH cookie (*i.e.*, all of the Web-based activity

engaged in via a mobile device) in its databases. If a person deleted the Turn third-party tracking cookie from her machine, Turn would simply wait until that same person sent another HTTP request to one of its partner sites, then place a new cookie on the user's machine, correlate the user's X-UIDH value with the cookie data it had already saved, and pick up tracking the person right where it had left off. This is ominously referred to by Turn as "respawning" the third-party tracking cookie, which led security experts to dub them "zombie" cookies. Nor could people thwart Turn through industry standard "do not track" settings, according to security analysts. Further still, because a mobile device sends HTTP requests through browsers *and* apps, Turn could use the embedded X-UIDH to correlate a user's conduct across *all* of her device's browsers and apps.

10. Thus, with these zombie cookies, Turn persistently and surreptitiously tracked all of users' Web-based activities without their knowledge or consent, and in disregard of users' efforts to prevent the tracking. Turn's surveillance, therefore, vastly eclipsed traditional methods of gathering user data.

11. Turn conducted its practices in secret. Notably, both before and after Defendant's behavior was brought to light by news reports and the investigation of an independent security researcher, Verizon took pains to assure its customers that it did not aid or sanction companies (such as Turn) using the X-UIDH to create persistent identifiers to covertly track them.

12. When first confronted about its practices, Turn stubbornly refused to accept that users' acts of deleting cookies clearly conveyed their desire not to have omnipresent, undeletable tracking cookies placed on their mobile devices again and again. Instead, Turn stated that it would continue "trying to use the most persistent identifier that we can in order to do what we do."

13. In a January 17, 2015 blog post, however, Turn stated that "[b]y early February, Turn will not 'respawn' cookie IDs associated with the Verizon UIDH." Max Ochoa, *'Zombie' Cookie ID to be suspended pending re-evaluation*, Turn (Jan. 17, 2015), https://www.turn.com/blog/zombie-cookie-id-to-be-suspended-pending-re-evaluation (last visited Mar. 23, 2015).

14. Turn's act of surreptitiously tracking people against their wishes, and of thwarting industry-standard consumer safeguards of privacy, is unconscionable. Based on Turn's own surveys, the overwhelming majority of Americans actively attempt to protect against the very practices in which Turn engaged. As Schneier notes:

> Today's technology gives governments and corporations robust capabilities for mass surveillance. Mass surveillance is dangerous. It enables discrimination based on almost any criteria: race, religion, class, political beliefs. It is being used to control what we see, what we can do, and, ultimately, what we say. It is being done without offering citizens recourse or any real ability to opt out, and without any meaningful checks and balances. It makes us less safe. It makes us less free. *Data and Goliath*, *supra*, at 3.

15. Turn's acts and omissions, complained of herein, are violations of N.Y. Gen. Bus. Law § 349 and amount to acts of trespass to chattels. Plaintiffs seek injunctive and declaratory relief, restitution, and statutory and monetary damages, individually and on behalf of a class of all persons in New York with a Verizon wireless data subscription at any time from 2012 to the present.

II. PARTIES

16. Plaintiff Anthony Henson is a resident of Rosedale, New York. He has been a Verizon mobile subscriber since 2002. During the relevant time period, Plaintiff subscribed to Verizon mobile cellular and data service for use with Internet-enabled smartphones, and he used his Verizon data plan to access Internet-based content multiple times a day through his smartphones' web browsers and applications. During the relevant time period, Plaintiff visited a variety of websites through his smartphones' web browsers, including those of Verizon, Microsoft, Stubhub, and Zales; visited news, email, sports, entertainment, commerce, social networking and search engines sites; and used a variety of common smartphone applications that obtain information through HTTP requests, including Facebook, Yahoo! Mail, YouTube, and Google Maps. In addition, during the relevant time period, Plaintiff Henson regularly deleted cookies and browsing history from his smartphones, typically once every couple of months, and, at times, more frequently. Plaintiff Henson was not made aware of and did not consent to Defendant's practices, as described in this Complaint.

17. Plaintiff William Cintron is a resident of Newburgh, New York and has been a Verizon mobile subscriber since 2013. During the relevant time period, Plaintiff Cintron subscribed to Verizon mobile cellular and data service for use with his Internet-enabled smartphone, and he used his Verizon data plan to access Internet-based content multiple times a day through his smartphone's web browsers and applications. During the relevant time period, Plaintiff visited a variety of websites through his smartphone's web browsers, including that of Verizon, DirecTV, Experian, and Microsoft; visited news, email, sports, entertainment, commerce, social networking and search engines sites; and used a variety of common smartphone applications that obtain information through HTTP requests, including Facebook, YouTube, Twitter, Tumblr, Engadget, Gmail, and Microsoft Outlook. In addition, during the relevant time period, Plaintiff Cintron regularly deleted cookies and browsing history from his smartphone, typically on a daily or weekly basis. Plaintiff Cintron was not made aware of, and did not consent to Defendant's practices as described in this Complaint.

18. Defendant Turn, Inc. is a Delaware corporation with its principal place of business in Redwood City, California.

19. Turn operates as an online advertising clearinghouse for companies such as Google, Yahoo and Facebook. When a user visits a website that contains Turn tracking code—which includes the websites of "300 of the world's top brands and media agencies," such as Accuen, Aegis, Amnet, Chrysler, Dentsu, DirecTV, Experian, Foursquare, Kraft, Kimberly-Clark, Microsoft, OMD, Progressive Insurance, StubHub, Thomas Cook, Toyota, Travelers, Verizon, VivaKi, and Zales—the company holds an auction within milliseconds for advertisers to target that user, and the highest bidder's ad instantly appears on the user's screen as the web page loads. *Turn Powers Dentsu's Data-Driven Marketing*, TURN (Oct. 13, 2014), http://www.turn.com/company/newsroom/turn-powers-dentsus-data-driven-marketing (last visited Mar. 23, 2015); *Turn Expands Premium Marketplace Offerings with New Mobile and Video Inventory Partners*, TURN (Jan. 22, 2015), http://www.turn.com/company/newsroom/turn-expands-premium-marketplace-offerings-with-new-mobile-and-video-inventory-partners (last visited Mar. 23, 2015). Turn says it receives 2 million requests for online advertising placements

per second. For these auctions to work, Turn needs to identify web users—and their browsing histories—through cookies. The cookies allow Turn to identify a user's web browsing habits, such as an interest in sports or shopping, which it uses to lure advertisers to the auction.

III. JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction of this action pursuant to 28 U.S.C. § 1332(d) and 1367 because this is a class action in which the matter or controversy exceeds the sum of $5,000,000, exclusive of interest and costs, and in which some members of the proposed Class are citizens of a state different from some defendants.

21. Venue is proper in this District because a substantial part of the events and omissions giving rise to Plaintiffs' claims occurred in this District and the Defendant resides in and transacts business in this District.

22. Pursuant to Civil L.R. 3-2(c), assignment to this Division is proper because a substantial part of the events and omissions which give rise to the claim occurred at Turn's headquarters in Redwood City, San Mateo County.

23. This Court has personal jurisdiction over Defendant because it transacts business in the United States, including in this District, has substantial aggregate contacts with the United States, including in this District, engaged and is engaging in conduct that had a direct, substantial, reasonably foreseeable and intended effect of causing injury to persons throughout the United States, and purposefully availed itself of the laws of the United States.

IV. FACTUAL ALLEGATIONS

A. "Cookies," Targeted Online Advertising, And The Tracking Of Users' Activity Across The Internet

24. Online advertising has grown in tandem with the use of the Internet generally, and commands an increasingly large market share. A recent industry report stated that the first half of 2014 saw an historic $23.1 billion in Internet ad revenue. *Digital Ad Revenues Hit Landmark High in First Half High of 2014*, IAB (Oct. 20, 2014), http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-102014 (last visited Mar. 23, 2014).

25. Much of the allure of online advertising lies in its ability to deliver targeted advertising—placing ads on websites that cater to the highly-specific behaviors or wants of an individual viewing a particular site. Targeted advertising is achieved by harvesting data about an individual, using the data to draw inferences about that individual's demographics and interests, and then serving up ads, promotions and messages based on those inferences.

26. One of the easiest ways to assemble data points is to observe an individual's web traffic (*i.e.*, the websites she visits). For example, a person who spends several minutes viewing shirts on a clothing brand's website is logically more likely to respond to an ad for that brand's shirts on other websites as that person continues to browse the Web, even days or months after first visiting the brand's website.

27. Because knowing where a person has been on the Web is instrumental to knowing what types of ads that individual might respond to, marketers created third-party tracking "cookies"—pieces of code that are transmitted from a website to an individual's web browser. As long as these cookies remain in the browser, they act as a beacon, transmitting that individual's Web browsing history back to the third party who first generated the cookie. These third-party tracking cookies stand in contrast to more benign first-party cookies—those associated with the website viewed by the user—which can, for example, perform functions like saving someone's preferences or login credentials for the next time the person visits the site.

28. As knowledge of third-party tracking cookies became public, citizens expressed profound discomfort at the idea of an unknown third party surreptitiously monitoring their online behavior in order to profit.

29. Indeed, the consequences of unknown third parties tracking and cataloging one's online activity have been an increasing focus not only of advocacy groups and pundits, but also academics. In a paper analyzing the prevalence of surreptitious third-party tracking cookie placement, the authors noted:

> Web browsing history is inextricably linked to personal information. The pages a user visits can reveal her location, interests, purchases, employment status, sexual orientation, financial challenges, medical conditions, and more. Examining individual page loads is often adequate to draw many conclusions

> about a user; analyzing patterns of activity allows yet more inferences.
>
> …
>
> Collection of sensitive personal information is not a hypothetical concern. In mid-2011, we discovered that an advertising network, Epic Marketplace, had publicly exposed its interest segment data, offering a rare glimpse of what third-party trackers seek to learn about users. User segments included menopause, getting pregnant, repairing bad credit, and debt relief. Several months later we found that the free online dating website OkCupid was sending to the data provider Lotame how often a user drinks, smokes, and does drugs. When Krishnamurthy et al. tested search queries on ten popular health websites, they found a third party learned of the user's query on nine of them. Jonathan R. Mayer & John C. Mitchell, *Third-Party Web Tracking: Policy and Technology*, 2012 IEEE Symposium On Security & Privacy 413, 415 (2012), *available at* http://www.academia.edu/2784919/Third-Party_Web_Tracking_Policy_and_Technology(last visited Mar. 23, 2015).

B. Standard Browser And Device Features For Blocking And Deleting Cookies

30. In light of widespread privacy concerns, major web browsers created features to allow users to delete cookies from their web sessions. *See, e.g.*, *Delete browsing, search and download history on Firefox*, MOZILLA, https://support.mozilla.org/en-US/kb/delete-browsing-search-download-history-firefox (last visited Mar. 26, 2015); *Manage your cookies and site data*, GOOGLE, https://support.google.com/chrome/answer/95647?hl=en&rd=1 (last visited Mar. 26, 2015); *Delete and manage cookies*, MICROSOFT, http://windows.microsoft.com/en-us/internet-explorer/delete-manage-cookies#ie=ie-11-win-7 (last visited Mar. 26, 2015); *Safari 5.1 (OS X Lion): Manage cookies*, APPLE, http://support.apple.com/kb/ph5042 (last visited Mar. 26, 2015). Indeed, most major browsers have implemented features to allow users to affirmatively and preemptively *block* cookies. *Id.*

31. Likewise, both computers and mobile devices have, as a standard feature, privacy settings enabling users to block and delete cookies from these devices.

32. Accordingly, while a reasonable person might expect third-party tracking cookies to be utilized on websites, it is equally understood that the person expects to be able to both *identify* those cookies and to elect *not* to be tracked by those cookies, should she wish, by either

(1) affirmatively blocking cookies from being placed on her browser, or (2) deleting cookies from her computer or mobile device.

33. In a 2013 white paper issued in conjunction with Forbes, Turn surveyed Americans' attitudes towards online tracking, marketing, and privacy. Forbes Insights, in association with Turn, *The Promise of Privacy: Respecting Consumers' Limits While Realizing the Marketing Benefits of Big Data*, Forbes (2013), *available at* http://images.forbes.com/forbesinsights/StudyPDFs/turn_promise_of_privacy_report.pdf. The results make clear that the overwhelming majority of Americans are not only concerned about their privacy, but also that the affirmative steps we take to guard our privacy are the *precise actions that Turn's acts and practices undermine*. Among the results:

- 69% of participants deleted cookies in order to "shield their online privacy;"
- 56% of participants "are generally uncomfortable with the amount of information companies know about them or could learn about them through their activities;" and
- 54% of participants felt that "their privacy concerns outweigh[ed] any benefits derived from sharing information with businesses." *Id. at 15, Insight Four: The Risk – and Cost – of Potential Privacy Missteps Cannot Be Overstated.*

34. Turn violated all of these reasonable expectations of privacy by creating zombie cookies that users could neither detect nor delete, and which monitored user behavior well beyond web browsing.

35. As Turn's business model could not survive without the surreptitious tracking of users across the web, it devised ways to make an end-run around users' cookie blocking and deleting technologies. Specifically, Turn seized on a unique and obscure routing feature utilized by the wireless service provider Verizon, which enabled Turn to alter fundamental properties of cookies so that the cookies would regenerate secretly on users' machines even after they had purportedly been cleared. As noted above, these cookies are referred to as "zombie" cookies, due

to their ability to regenerate and continue to track users despite their wishes, actions, and best efforts not to be tracked.

C. Turn's End-Run Around Industry-Standard Consumer Privacy Protections Through Exploitation Of The X-UIDH And Placement Of Zombie Cookies

36. Turn thwarts industry-standard consumer privacy protections with its zombie cookie and its exploitation of Verizon's X-UIDH.

37. Turn's practices depend on HTTP requests—a basic feature of Internet communications—and the information embedded in those requests.

38. A user's device will send an HTTP request to the server for the website she is trying to view; it is essentially a request for information related to the website. For example, when an individual wants to view the New York Times' website, she types www.nytimes.com into her phone's web browser; the web browser then sends an HTTP request to the New York Times' server associated with the address www.nytimes.com; and the server then sends data back to the individual's web browser, which enables her to view the newspaper's website.

39. The HTTP request will typically have a variety of header fields, or information embedded in the request that describes the nature of the request and the device making the request. Among those headers is the "referrer" (often spelled in Internet parlance as "referer"), which is used to describe where or how the request was generated. Typically, a referrer describes the previous website from which the request was made – *i.e.*, when one visits website A and clicks on a link to website B, the HTTP request sent to website B's server will contain a referrer field showing that the request came from website A. However, referrer fields can also be used to describe the specific computer sending the HTTP request, as is the case in the instant matter.

40. Beginning in 2012, Verizon began injecting a particular referrer header into all HTTP requests from the mobile devices of its customers, whether the request was from the device's browser or one of its applications. This referrer header is called the "unique identifier header" ("UIDH" or "X-UIDH"). Each Verizon customer has her own unique X-UIDH value. Thus, the X-UIDH could allow the website (or any other party with access to the HTTP request) to uniquely identify the user and device transmitting the HTTP request.

41. The Electronic Frontier Foundation (the "EFF"), a leading nonprofit organization that defends civil liberties in the digital world, issued a report in November 2014 detailing how exploiting Verizon's X-UIDH could enable a company—such as Turn—to create zombie cookies that (1) were undiscoverable to users; and (2) could never be deleted or even protected against by the user. Per the EFF, the X-UIDH "functions even if you use a private browsing mode or clear your cookies."

> Also …[the X-UIDH] is nearly invisible to the user and can't be seen or changed in the device's browser settings. If a user clears their cookies, the [X-UIDH] remains unchanged. Worse, ad networks can immediately assign new cookies and link them to the cleared cookies using the unchanged X-UIDH value.…To compound the problem, the header also affects more than just web browsers. Mobile apps that send HTTP requests will also have the header inserted. This means that users' behavior in apps can be correlated with their behavior on the web, which would be difficult or impossible without the header. Jacob Hoffman-Andrews, *Verizon Injecting Perma-Cookies to Track Mobile Customers, Bypassing Privacy Controls*, Electronic Frontier Foundation (Nov. 3, 2014), https://www.eff.org/deeplinks/2014/11/verizon-x-uidh (last visited Mar. 23, 2015) (emphasis added).

42. The EFF reported on what a company *could*, in theory, do; Stanford professor and security expert Jonathan Mayer revealed that this is precisely what Turn, in fact, *did*. Jonathan Mayer, *The Turn-Verizon Zombie Cookie*, Web Policy, (Jan. 14, 2015), http://webpolicy.org/2015/01/14/turn-verizon-zombie-cookie/#turn_verizon_fn 2 (last visited Mar. 23, 2015). Professor Mayer's forensic analysis found Turn (i) creating third-party tracking cookies that latched onto Verizon customers' X-UIDH, (ii) tracking unsuspecting users' browsing habits on their mobile devices, and (iii) creating a zombie cookie that cataloged the entirety of users' activity on their mobile devices, even if users sought to protect their privacy by clearing cookies on their devices. Professor Mayer's research also revealed that users could neither detect nor erase such zombie cookies.

43. Specifically, Turn monitored the web traffic of its partner websites, searching the headers of HTTP requests for Verizon customers (and the attendant X-UIDH embedded in the request). Upon receiving such requests, Turn would check the X-UIDH value in the current HTTP request against a database of values that it had stored from previous cookies. If there was a

match—and even if the Verizon customer had previously cleared her machine of old cookies in an effort to not be tracked—Turn would then place a new cookie on the Verizon customer's machine that contained all of the values from the old cookies in its database that were associated with the same X-UIDH.

44. This practice enables Turn to tie a user's deleted browsing history (associated with the old, cleared cookie) with the current browsing history, *thus persistently and surreptitiously tracking the customer across the Web*, against her express wishes.

45. Professor Mayer documented his analysis, identifying Turn as an offender, with screenshots of Turn's code and step-by-step explanations of Turn's brazen attempts to capitalize on Verizon protocols in order to track users:

> Confirmation was easy. A request to certain Turn resources, sans Verizon header, simply drops a uid cookie.
>
> $ curl -D - "http://ad.turn.com/server/ads.js" ... Set-Cookie: uid=2415230717135370700; Domain=.turn.com; ...
>
> Each cookieless request results in a new ID.
>
> $ curl -D - "http://ad.turn.com/server/ads.js" ... Set-Cookie: uid=4425321986559530189; Domain=.turn.com; ...
>
> So far, no surprises. When requests include a Verizon header, though, the subsequent response behavior is different.
>
> $ curl -H "X-UIDH: OTgxNT..." -D - "http://ad.turn.com/server/ads.js" ... Set-Cookie: uid=4012847891611109688; Domain=.turn.com;... $ curl -H "X-UIDH: OTgxNT..." -D - "http://ad.turn.com/server/ads.js" ... Set-Cookie: uid=2539356028667362074; Domain=.turn.com;... Set-Cookie: uid=4012847891611109688; Domain=.turn.com;...
>
> As before, there's a new ID. But a second Set-Cookie header appears; it trumps the first header and restores the old ID…[3] I tried moving between IP addresses and User-Agents, in case those factored into Turn's behavior. The zombie cookie remained. *Id.*

46. To summarize, when a Turn partner website received an HTTP request from a Verizon device, the Turn cookie latched on to the X-UIDH (4012847891611109688), and persistently identified the device as being associated with the X-UIDH.

47. Turn's practice of using the X-UIDH identifier as a beacon to track users' browsing habits extends beyond Turn's affiliate websites to *additional* third parties:

> Turn's zombie cookie was sent to or from over thirty other businesses. They included Google, Facebook, Yahoo, Twitter, Walmart, and WebMD. How those firms use Turn's ID, I can't say—it's entirely possible that some unknowingly tracked users with a zombie value. They certainly possessed sufficient information. It's especially likely for businesses that dropped their own tracking cookie with Turn's ID.
>
> . . .
>
> In sum, there are widespread collateral consequences from Turn's zombie cookie. *Id.*

48. As the above paragraphs describe, Turn knowingly inserted code—in the form of X-UIDH-augmented zombie cookies—onto the devices of Plaintiffs and Class members, exploiting a routing feature inherent to Verizon's infrastructure. It did so in order to disable the standard privacy controls employed by individuals (such as deleting or blocking cookies), thereby enabling it to surreptitiously observe and catalog any and all online activity of Plaintiffs and Class members.

D. Turn's Surreptitious Monitoring Of The Entirety Of User Activity On Mobile Devices

49. While Turn's zombie cookies enabled it surreptitiously and persistently to track users' Internet presence via their Web browser history, they also enabled Turn to look at other user behaviors related to their mobile devices, generally.

50. Unlike our activity on traditional computers, where we connect to sites using a single Web browser that can be easily tracked by cookies, Americans on smartphones and tablets also employ many different apps that do not share information with each other, or with the user's Web browser.

51. For instance, a person may browse specific websites on the Internet using her phone's Web browser, but may then use a dedicated app on her smartphone to access specific content (*e.g.*, using the New York Times' app to view articles, the Netflix app to stream movies, or the Bank of America app to check an account balance). When a person utilizes an app to

access Internet content, the app does not use the mobile device's browser, but instead uses a WebView—a browser unique to the app that displays Internet content in the app. This creates what is known as a "sandbox" environment for each app, meaning that each app functions uniquely on a mobile device, and that cookies placed on the device's Web browser do not track user behavior in a given app. Similarly, cookies associated with a given app do not track user interactivity with another app, due to the sandbox environment.

52. Thus, on a mobile device, any attempt to use cookies to create user profiles should be compartmentalized: one may be tracked through usage of the Web browser or tracked through usage of an app, but never through usage of both. Beyond serving a privacy purpose, sandboxing serves a security function. As Apple explains: "[The] App sandbox provides a last line of defense against the theft, corruption, or deletion of user data if an attacker successfully exploits security holes in your app or the frameworks it is linked against." Apple, *About App Sandbox*, Mac Developer Library, https://developer.apple.com/library/mac/documentation/Security/Conceptual/AppSandboxDesignGuide/AboutAppSandbox/AboutAppSandbox.html (last updated Feb. 11, 2014).

53. Thus, a person does not reasonably expect that a third-party tracking cookie can or will monitor *all* activity on a mobile device, and instead only expects to be tracked (1) via the smartphone's Web browser *or* (2) via app-specific cookies (but never both in conjunction) and (3) in such a manner that can be guarded against using the smartphone's standard privacy settings for blocking and deleting cookies.

54. However, because of the manner in which Turn reconfigured its third-party tracking cookies to latch onto the X-UIDH in all Verizon HTTP requests, Turn was thus able to monitor—and correlate—all user activity on the mobile devices, where an HTTP request was sent. Thus, Turn's undisclosed practices enabled it to create profiles that included both browsing history and app engagement. As a result, Turn could and did create much more revealing—and potentially lucrative—pictures of the targeted users, without the persons' knowledge or consent.

E. Turn's Failure To Disclose Its Practices And Deceptive Omissions

55. Turn designed its zombie cookie to circumvent a person's efforts to avoid being tracked and profiled. When confronted with allegations that it was taking advantage of unique features of Verizon's protocols in order to profile users, Turn offered a tone-deaf response, doubling down on its wrongful behavior and stating that it was "*trying to use the most persistent identifier that we can in order to do what we do*" (emphasis added). Julia Angwin and Mike Tigas, *Zombie Cookie: The Tracking Cookie That You Can't Kill*, ProPublica (Jan. 14, 2015), http://www.propublica.org/article/zombie-cookie-the-tracking-cookie-that-you-cant-kill (last visited Mar. 23, 2015).

56. When pushed on this point, Turn stated that it refused to consider the act of clearing third-party tracking cookies as a signal that users want to opt out from being tracked. "*There are definitely people who feel that if they clear their cookies, they won't be tracked, **and that is not strictly accurate***," said Joshua Koran, senior vice president of product management at Turn. (Emphasis added). *Id*.

57. In its official statement, issued in response to public outcry as news of the zombie cookies came to light, Turn simply stated that "clearing cookies is not a reliable way for a user to express their desire not to receive tailored advertising." Julia Angwin and Mike Tigas, *Zombie Cookies Slated to be Killed*, ProPublica (Jan. 16, 2015), http://www.propublica.org/article/zombie-cookies-slated-to-be-killed (last visited Mar. 23, 2015) (emphasis added).

58. This statement flies in the face of Turn's own published research, however, as illustrated in paragraph 33, *supra*. Turn's justifications for its practices demonstrate a clear contempt for user privacy, and an intent to willingly disregard a reasonable person's attempt to protect her privacy.

59. No reasonable means are available to avoid or decline Turn's cookies in the first instance. While Turn does purport to allow users to opt-out of receiving targeted advertising, it requires users to go to Turn's website and place an "opt-out" cookie onto their computer or mobile device. Notably, the opt-out cookie does not prevent people from being tracked, and it

does not prevent Turn from respawning deleted cookies; rather, it only determines whether the tracked individual will see targeted advertising. Thus, even if a privacy-conscious person knew of Turn's existence, knew that Turn purported to offer an opt-out cookie on its website, and sought to opt out of being tracked by X-UIDH zombie cookies—and was assured by Turn that *she had* opted out—Turn continued to monitor and record that person's online behavior, and to respawn its third-party tracking cookies at will. In effect, a person who wished not to be profiled by Turn had no true recourse.

60. Turn's practices were not only undertaken without the knowledge or consent of users, they may also have been undertaken without the knowledge or consent of Verizon or, on information and belief, any of Turn's partner websites. While Turn had entered into advertising partnerships with Verizon, its aggressive use of the X-UIDH to create zombie cookies was undertaken without Verizon's approval.

61. Verizon assured customers that the X-UIDH would not be used by advertising partners for tracking and profiling purposes by dismissing the possibility that "that sites and ad entities will attempt to build customer profiles" using its identifiers. Julia Angwin and Mike Tigas, *Zombie Cookie: The Tracking Cookie That You Can't Kill*, ProPublica (Jan. 14, 2015), http://www.propublica.org/article/zombie-cookie-the-tracking-cookie-that-you-cant-kill (last visited Mar. 23, 2015).

62. A Verizon technology director who helped develop the technology behind the X-UIDH recently stated that the technology was not intended for use by other companies to remember its subscribers or recover information about them. When asked about Turn's use of the X-UIDH to create a zombie cookie for profiling purposes, Mr. Atreya disavowed Turn's behavior: "[Turn] did not talk to me. If they did, I would not have been satisfied." Natasha Singer and Brian X. Chen, *Verizon's Mobile 'Supercookies' Seen as Threat to Privacy*, N.Y. Times (Jan. 25, 2015), http://www.nytimes.com/2015/01/26/technology/verizons-mobile-supercookies-seen-as-threat-to-privacy.html?ref=technology&_r= 1 (last visited Mar. 23, 2015).

63. Verizon has issued a statement disclaiming knowledge or responsibility for Turn's use of the X-UIDH to create zombie cookies on mobile devices:

> Recent news reports have raised concerns about how TURN is using the [X-UIDH] for purposes outside of Verizon's advertising programs. TURN has announced its intent to discontinue this practice and we will work with other partners to ensure that their use of [the X-UIDH] is consistent with the purposes we intended. *Verizon Wireless' Use of a Unique Identifier Header (UIDH) [FAQ]*, Verizon Wireless, https://www.verizonwireless.com/support/unique-identifier-header-faqs/ (last visited Mar. 23, 2015).

64. Turn had a duty to disclose its practices to users given its exclusive knowledge of, and/or superior knowledge regarding, the material fact that it was tracking Plaintiffs and Class members using zombie cookies, which could not be detected, declined, or deleted. Turn further had a duty to disclose the fact that its zombie cookies were capable of monitoring the entirety of a user's activity on her mobile device.

65. Turn's exploitation of the X-UIDH to secretly track Americans' online activities evinces a disregard for user privacy and user choice, and violates consumer protection laws and common law guarantees of privacy.

F. Fraudulent Concealment and Tolling

66. The applicable statutes of limitation are tolled by virtue of Turn's knowing and active concealment of the facts alleged above. Plaintiffs and Class members were ignorant of the information essential to the pursuit of these claims, without any fault or lack of diligence on their own part.

67. At the time this action was filed, Turn was under a duty to disclose the true character, quality, and nature of its activities to Plaintiffs and the Class. Turn is therefore estopped to rely on any statute of limitations.

68. Turn's fraudulent concealment is common to the Class.

V. CLASS ALLEGATIONS

69. Plaintiffs bring this action under Rule 23 of the Federal Rules of Civil Procedure, on behalf of themselves and the following Class: all persons in New York who subscribed to a Verizon wireless data plan at any time from 2012 to the present. Based on currently available information, Plaintiffs understand that Turn began the alleged practices some time in 2012. The

exact date will be determined through discovery and the class definition will be refined accordingly.

70. **Numerosity (Rule 23(a)(1)):** Individual joinder is impracticable. Verizon has approximately 125 million mobile subscribers in the United States that Turn was able to secretly track using the X-UIDH. Accordingly, the number of persons in the Class is likely in the many thousands or millions.

71. **Commonality (Rule 23(a)(2))**: Numerous questions of law and fact are common to the claims of the Plaintiffs and members of the proposed Class. These include:

a. Whether Turn used the X-UIDH to place its own cookies on Class members' mobile devices;

b. Whether Turn used the X-UIDH to recreate cookies that Class members had previously deleted from their mobile devices;

c. Whether Turn used the X-UIDH to link browsing histories to usage histories in sandboxed apps;

d. Whether Turn used the X-UIDH, cookies, or any other mechanism to (i) secretly track, compile, and/or record users' browsing habits; (ii) build profiles or dossiers of users; and (iii) use information obtained through these mechanisms for Turn's own commercial gain, by selling the information to advertisers;

e. Whether Turn failed to disclose its use of the tracking and profiling mechanisms described above;

f. Whether Turn violated N.Y. Gen. Bus. Law § 349;

g. Whether Plaintiffs and Class members are entitled to statutory and other damages, compensatory damages, civil penalties, punitive or multiple damages, restitution, declaratory relief, injunctive relief, or other equitable relief.

h. Whether Turn has unlawfully profited from its conduct, and whether it must disgorge or restore its ill-gotten profits; and

72. **Typicality (Rule 23(a)(3)):** Plaintiffs' claims are typical of the claims of the members of the proposed Class. The factual and legal bases of Defendant's liability to Plaintiffs

and other members of the proposed Class are the same and resulted in injury to Plaintiffs and all of the Class members.

73. **Adequacy (Rule 23(a)(4)):** Plaintiffs will represent and protect the interests of the proposed Class both fairly and adequately. They have retained counsel competent and experienced in complex class action litigation. Plaintiffs have no interests that are antagonistic to those of the proposed Class, and their interests do not conflict with the interests of the proposed Class members they seek to represent.

74. **Predominance and Superiority (Rule 23(b)(3)):** This proposed class action is appropriate for certification. The common issues identified above will predominate over any individual ones. Class proceedings on these facts and this law are superior to all other available methods for the fair and efficient adjudication of this controversy, given that joinder of all members is impracticable. Even if members of the proposed Class could sustain individual litigation, that course would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex factual and legal controversies present in this controversy. Here, the class action device will present far fewer management difficulties, and it will provide the benefit of a single adjudication, economies of scale, and comprehensive supervision by this Court. Further, uniformity of decisions will be assured.

VI. CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF

N.Y. GEN. BUS. LAW § 349

75. Plaintiffs reallege and incorporate by reference all paragraphs as though fully set forth herein.

76. Plaintiffs and Class members are "persons" within the meaning of New York General Business Law § 349(h).

77. Turn is a "person," "firm," "corporation," or "association" within the meaning of N.Y. Gen. Bus. Law § 349.

78. Section 349 makes unlawful "[d]eceptive acts or practices in the conduct of any business, trade or commerce."

79. Turn's conduct constitutes "deceptive acts or practices" within the meaning of N.Y. Gen. Bus. Law § 349.

80. Turn's conduct occurred in the conduct of trade or commerce, and was directed at consumers.

81. Turn's conduct was misleading in a material way, because Turn (1) exploited the X-UIDH in order to install zombie cookies on the mobile devices of Class members without their knowledge or consent; (2) recreated deleted cookies on the mobile devices of Verizon subscribers without their knowledge or consent; (3) circumvented mobile device settings, including browser settings, used to prevent the placement of third-party tracking cookies on the device or tracking of the user's web browsing; (4) tracked and compiled Class members' web browsing histories—and sandboxed in-app activities—without their knowledge or consent, including any personal, private, and confidential data used during or revealed by the Class members' browsing; and (5) used Class members' personal, private, and confidential data for commercial gain without their knowledge or consent.

82. As a result of Turn's deceptive acts and practices, Plaintiffs and Class members were injured and damaged in that they suffered a loss of privacy through the tracking and collection of their personal and private information; were denied use of the privacy controls and settings on their mobile devices, including the ability to clear or delete third-party tracking cookies and browsing history; had their devices persistently infected with zombie cookies they could not delete or remove; and had their personal and confidential information used by Turn for its own commercial gain without the consumers' knowledge or consent.

83. Because Turn's willful and knowing conduct caused injury to Plaintiffs and Class members, the Class seeks recovery of actual damages or $50, whichever is greater, discretionary treble damages up to $1,000, punitive damages, reasonable attorneys' fees and costs, an order enjoining Turn's deceptive conduct, and any other just and proper relief available under N.Y. Gen. Bus. Law § 349.

SECOND CLAIM FOR RELIEF

TRESPASS TO CHATTELS

84. Plaintiffs reallege and incorporate by reference all paragraphs as though fully set forth herein.

85. By engaging in the acts alleged in this Complaint, Turn intentionally, and without justification or consent, physically interfered with the use and enjoyment of personal property in the possession of Plaintiffs and Class members, thereby causing them harm.

86. Plaintiffs and Class members are or were the owners and/or possessors of mobile devices that operate or operated on Verizon's cellular network during the relevant time period, and upon which Turn placed its zombie cookies.

87. Turn dispossessed Plaintiffs and Class members of the use of their mobile devices, or parts of them, for a substantial time by commandeering the resources of the mobile devices for Turn's own purposes, and by deploying zombie cookies to said devices, thereby invading the privacy of Plaintiffs and Class members and damaging the privacy controls of Plaintiffs and Class members' mobile devices.

88. Turn impaired the condition, quality, and value of the mobile devices of Plaintiffs and Class members through the installation of its zombie cookies, which constituted an ongoing alteration to the mobile devices of Plaintiffs and Class members, circumventing privacy controls in said devices and causing said devices to transmit information to Turn to which Turn was not entitled.

89. Plaintiffs and Class members have had, at all times relevant to this litigation and continuing to present day, a legally protected economic interest and a privacy interest in their personal information including, but not limited to, the activity they engage in on their mobile devices, which Turn caused to be transmitted to itself via its zombie cookies.

90. Turn engaged in acts of deception and concealment in order to gain access to the personal information contained in and transmitted by the mobile devices of Plaintiffs and Class members.

91. Turn's acts and practices – impairing the condition, quality, and value of the mobile devices of Plaintiffs and Class members through the installation of its zombie cookies – was done without the consent of Plaintiffs and Class members.

92. Turn's acts and practices – impairing the condition, quality, and value of the mobile devices of Plaintiffs and Class members through the installation of its zombie cookies – caused real and substantial damage to Plaintiffs and Class members.

93. Plaintiffs, individually and on behalf of the Class, seek injunctive relief restraining Turn from resuming its acts and practices complained of herein, and enjoining Turn to purge the data thus far retained in association with Plaintiffs and Class members. Plaintiffs additionally seek damages individually and on behalf of the Class.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, pray for judgment against Defendant and that the Court may:

a) Certify this case as a class action on behalf of the Class defined above, appoint Plaintiffs as Class representatives, and appoint Plaintiffs' counsel as Class counsel;

b) Declare that Defendant's actions, as set forth above, violate N.Y. Gen. Bus. Law § 349, and amount to acts of trespass to chattels;

c) Award injunctive and equitable relief as applicable to the Class, including:

i. Prohibiting Defendant from resuming the acts complained of herein;

ii. Requiring Defendant to provide reasonable notice and choice to users regarding Defendant's data collection, profiling, retention, and opt-out practices;

iii. Requiring Defendant to disgorge to Plaintiffs and Class members all of Defendant's ill-gotten gains; and

iv. Requiring Defendant to delete all data from and about Plaintiffs and Class members that it collected as a result of the acts complained of herein.

d) Award damages, including statutory and treble damages where applicable, to Plaintiffs and Class members in an amount to be determined at trial;

e) Award restitution against Defendant for all money to which Plaintiffs and Class members are entitled in equity;

f) Award Plaintiffs and Class members their reasonable litigation expenses and attorneys' fees, including pre- and post-judgment interest to the extent allowable; and

g) All other relief as this Court deems just and proper.

Dated: April 1, 2015

Respectfully submitted,

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP

By: _____
Michael W. Sobol

Michael W. Sobol (CA 194857)
msobol@lchb.com
Nimish R. Desai (CA 244953)
ndesai@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: 415.956.1000
Facsimile: 415.956.1008

Nicholas Diamand
ndiamand@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
250 Hudson Street, 8th Floor
New York, NY 10013-1413
Telephone: 212.355.9500
Facsimile: 212.355.9592

Hank Bates (CA 167688)
hbates@cbplaw.com
CARNEY BATES & PULLIAM PLLC
11311 Arcade Drive, Suite 200
Little Rock, AR 72212
Telephone: 501.312.8500

Bradley S. Clanton
brad@clantonlegalgroup.com
CLANTON LEGAL GROUP PLLC
627 Mohawk Avenue
Jackson, MS 39216
Telephone: 601-454-8794
Facsimile: 866-421-9918

Attorneys for Plaintiffs and the Proposed Class

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury.

Dated: April 1, 2015

Respectfully submitted,

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP

By: _____
Michael W. Sobol

Michael W. Sobol (CA 194857)
msobol@lchb.com
Nimish R. Desai (CA 244953)
ndesai@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: 415.956.1000
Facsimile: 415.956.1008

Nicholas Diamand
ndiamand@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
250 Hudson Street, 8th Floor
New York, NY 10013-1413
Telephone: 212.355.9500
Facsimile: 212.355.9592

Hank Bates (CA 167688)
hbates@cbplaw.com
CARNEY BATES & PULLIAM PLLC
11311 Arcade Drive, Suite 200
Little Rock, AR 72212
Telephone: 501.312.8500

Bradley S. Clanton
brad@clantonlegalgroup.com
CLANTON LEGAL GROUP PLLC
627 Mohawk Avenue
Jackson, MS 39216
Telephone: 601-454-8794
Facsimile: 866-421-9918

Attorneys for Plaintiffs and the Proposed Class