UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

San Francisco Division

ANTHONY HENSON, et al.,

Plaintiffs,

v.

TURN, INC.,

Defendant.

Case No. 15-cv-01497-JSW (LB)

ORDER ADJUDICATING DISCOVERY DISPUTE REGARDING REQUESTS FOR (1) INSPECTION OR FORENSIC IMAGES OF MOBILE DEVICES, (2) WEB BROWSING HISTORY, AND (3) COOKIES

Re: ECF No. 87, 90

INTRODUCTION

Plaintiffs Anthony Henson and William Cintron, subscribers to Verizon's cellular and data services, bring this data-privacy class action against defendant Turn, Inc. The plaintiffs' allegations center around "cookies": lines of software code that monitor and gather information about users' browsing and app use. Web browsers, computers, and mobile devices have settings that allow users to block or delete cookies from their devices. The plaintiffs allege Turn engaged in a practice of placing so-called "zombie cookies" on users' devices: cookies that users either cannot delete or block or that, when users try to delete them, "respawn" to continue tracking users across the web. The plaintiffs, both New York residents, bring claims for (1) violations of New York General Business Law § 349, which makes unlawful "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in [New York]," and (2) trespass to chattels.

Turn issued a number of discovery requests for production ("RFPs") to the plaintiffs. Among other things, Turn requested that the plaintiffs (1) produce their mobile devices for inspection or produce complete forensic images of their devices (RFP 1), (2) produce their full web browsing history from their devices (RFP 32), and (3) produce all cookies stored on or deleted from their devices (RFP 33).[1] The plaintiffs argue that Turn's requests are overbroad and invade their privacy rights. The plaintiffs propose instead that they produce (1) their web browsing history and cookies associated with Turn partner websites (contingent on Turn's identifying such sites) and (2) the date fields (but not the content) of all other cookies on their mobile devices.[2] The plaintiffs oppose allowing Turn to inspect their devices or producing complete forensic images of their devices.[3]

Judge White referred all discovery matters to the undersigned.[4] The undersigned can decide the parties' dispute without a hearing. N.D. Cal. Civ. L.R. 7-1(b). For the following reasons, the undersigned adopts the plaintiffs' proposals, as slightly modified below.

STATEMENT

1. The Plaintiffs' Allegations

Users increasingly use a single mobile device — a smartphone or a tablet — for their online activities, including web browsing, reading the news, listening to radio content, accessing their banking information and managing their finances, shopping online, using GPS for directions and traffic updates, communicating over email and social networks, and reading sites like WebMD to assess their medical condition.[5] Marketing companies like Turn have developed ways to place

[1] Joint Letter Br. – ECF No. 90 at 2–5; Joint Letter Br. Ex. 1 – ECF No. 90-1. (The parties filed two copies of the letter brief, one at ECF No. 87 without an exhibit, and one at ECF No. 90 with an exhibit containing RFPs 1, 32, and 33, and the plaintiffs' responses thereto. Other than the exhibit, the letters are identical.) Citations refer to material in the Electronic Case File ("ECF"); pinpoint citations are to the ECF-generated page numbers at the top of documents.

[2] Joint Letter Br. – ECF No. 90 at 8–9.

[3] *Id.* at 7.

[4] Referral Order – ECF No. 88.

[5] Compl. – ECF No. 1 at 3 (¶¶ 2–3).

"tracking beacons" on these devices — lines of code called "cookies" — through web browsers or other smartphone apps.[6] Cookies monitor and gather information about a user's website browsing and app use, which includes personal information regarding the user's daily routines.[7] The resulting data is analyzed and used to target advertisements that match the user's profile.[8]

Consumers have expressed discomfort at the idea of an unknown third party surreptitiously monitoring their online activity for commercial purposes.[9] As one academic study reported:

> 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. . . . 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.[10]

In a 2013 white paper issued in conjunction with Forbes, Turn surveyed Americans' attitudes about online tracking, marketing, and privacy.[11] The survey found that, among other things, 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

---

[6] *Id.* at 3 (¶ 3), 9 (¶ 27).

[7] *Id.* at 3 (¶ 3).

[8] *Id.* at 3 (¶ 3), 9 (¶¶ 25–27).

[9] *Id.* at 3–4 (¶ 4), 9 (¶ 28).

[10] *Id.* at 9–10 (¶ 29) (citing Jonathan R. Mayer & John C. Mitchell, *Third-Party Web Tracking: Policy and Technology*, 2012 IEEE Symposium on Security & Privacy 413, 415 (2012)).

[11] *Id.* at 11 (¶ 33) (citing Forbes, *The Promise of Privacy: Respecting Consumers' Limits While Realizing the Marketing Benefits of Big Data* (2013) (*The Promise of Privacy*), *available at* http://images.forbes.com/forbesinsights/StudyPDFs/turn_promise_of_privacy_report.pdf (last visited Oct. 22, 2018)).

outweigh[ed] any benefits derived from sharing information with businesses."[12] In light of privacy 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.[13]

Turn developed a method that allegedly made an "end-run" around users' cookie-blocking-and-deleting technologies.[14] Turn allegedly did so through a Verizon function that created a persistent, unique identifier header ("UIDH" or "X-UIDH") for Verizon subscribers.[15] Each Verizon customer had a unique X-UIDH value.[16] Verizon embedded that unique X-UIDH value into the header of every HTTP request that its customers made from their mobile devices.[17] Turn monitored the web traffic of its partner websites, searching for HTTP requests from Verizon customers (and the attendant X-UIDH values embedded in the requests).[18] Upon receiving an HTTP request, Turn would check the X-UIDH value in the request against a database of values that it had stored from previous cookies.[19] If there was a match, Turn would place a new cookie on the user's device that contained all of the values from the old cookies in its database that were associated with the same X-UIDH — even if the user had previously deleted cookies from her device in an effort to not be tracked.[20] Turn refers to this as "respawning," which led security

---

[12] *Id.* (citing *The Promise of Privacy* at 15).

[13] *Id.* at 4 (¶ 5), 10 (¶¶ 30–31).

[14] *Id.* at 11 (¶ 35).

[15] *Id.* at 4 (¶¶ 7–8), 13 (¶ 43).

[16] *Id.* at 12 (¶ 40).

[17] *Id.* An "HTTP request" is a request from a device to a web server for the website that a user is trying to view. *Id.* (¶ 38). For example, if a user wants to view the New York Times's website and types www.nytimes.com into her phone's web browser, the web browser sends an HTTP request to the Times's web server at http://www.nytimes.com. *Id.* The server then sends data back to the user's web browser, which enables the user to view the Times's website. *Id.*

[18] *Id.* at 13 (¶ 43).

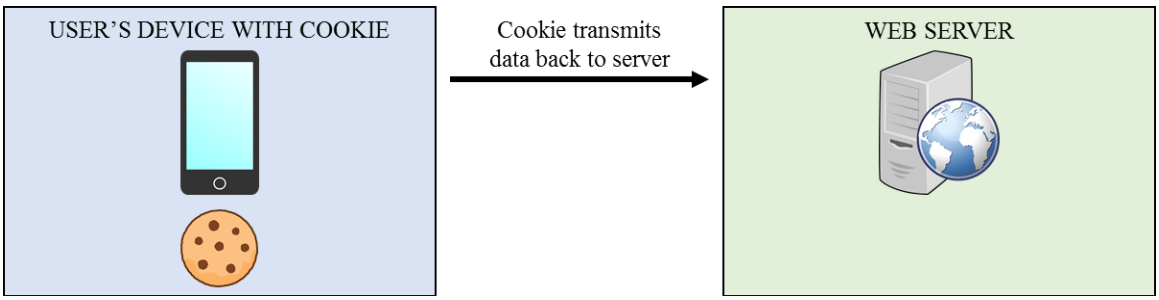
[19] *Id.*

[20] *Id.* at 13–14 (¶ 43).

experts to refer to these cookies as "zombie cookies" because they have the ability to regenerate and continue to track users despite users' attempts to not be tracked.[21]

The plaintiffs alleged the following example of this process at work, citing in part an analysis conducted by Stanford professor Jeremy Mayer.[22] Without a Verizon X-UIDH, when a user visits a Turn partner website, the website might place a cookie in her browser with a certain ID number (the example ID number used in the complaint of the cookie placed in the user's browser was 2415230717135370700).[23]

As long as the cookie remains in the browser, it allegedly transmits the user's browsing history back to the third party that first generated the cookie.[24]



[21] *Id.* at 5 (¶ 9), 11–12 (¶ 35).

[22] *Id.* at 13–15 (¶¶ 42–47) (citing Jonathan Mayer, *The Turn-Verizon Zombie Cookie*, Web Policy (Jan. 14, 2015), http://webpolicy.org/2015/01/14/turn-verizon-zombie-cookie (last visited Oct. 22, 2018)).

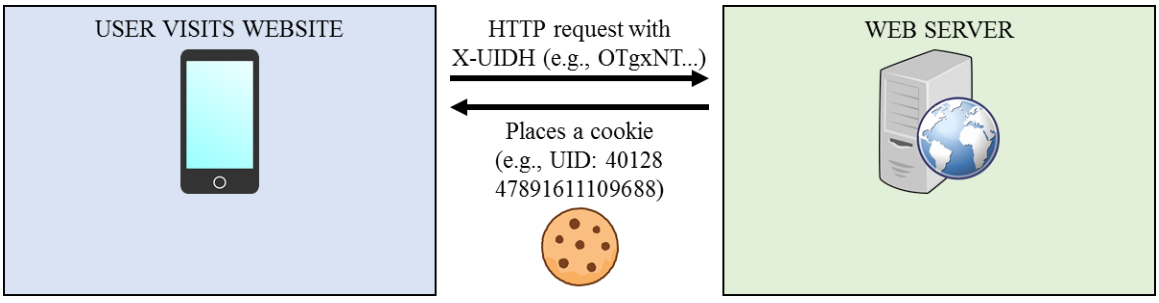
[23] *Id.* at 14 (¶ 45). The ID numbers used here are the ones used in Professor Mayer's analysis and cited in the plaintiffs' complaint.

[24] *Id.* at 9 (¶ 27).

If the user then deletes her cookies:

and then visits another Turn partner website, the website would place a new cookie in her browser with a new ID number (the new example ID number used in the complaint was 4425321986559530189).[25]

With a Verizon X-UIDH, however, when a user visits a Turn partner website, the website might place a cookie in her browser with a certain ID number (the example X-UIDH used in the complaint was "OTgxNT...," and the example ID number of the cookie placed in the user's browser was 4012847891611109688).[26]

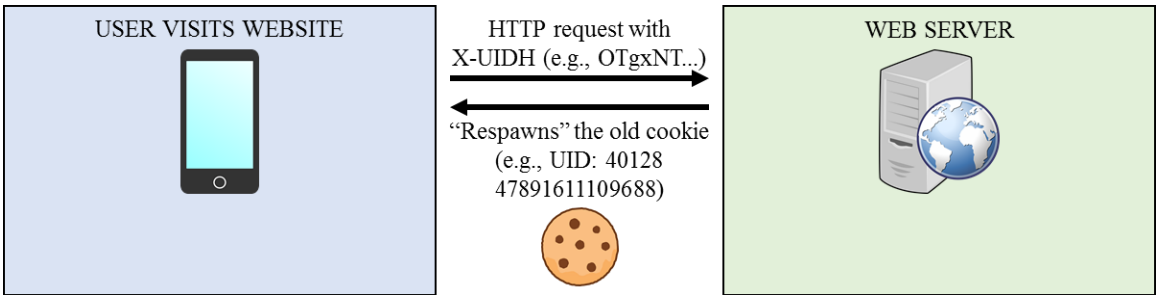


[25] *Id.* at 14 (¶ 45).

[26] *Id.* The complaint characterizes 4012847891611109688 as the Verizon X-UIDH in Professor Mayer's example, *id.* (¶ 46), but Professor Mayer's article shows that the Verizon X-UIDH in his example is actually OTgxNT..., and 4012847891611109688 is an ID number that is set in the cookie placed in the user's browser.

If the user then deletes her cookies:

and visits another Turn partner website, the website recognizes the Verizon X-UIDH and places a cookie in her browser with the same ID as before and all of the values from the user's old cookie that Turn stored within its database.[27]



2. The Parties' Discovery Dispute

The parties raise disputes with respect to three of Turn's requests for production: RFP 1, RFP 32, and RFP 33.[28] RFP 1 is a request for the plaintiffs to produce "[a]ll mobile devices with which You accessed the internet via the Verizon network during the alleged Class Period" (or complete forensic images of the devices).[29] RFP 32 is a request for the plaintiffs to produce "[a]ll data from each Mobile Device reflecting or regarding the user's web browsing history, including web pages viewed either through a dedicated browser application or an 'in-app' browser embedded in another type of application."[30] RFP 33 is a request for the plaintiffs to produce "[a]ll data from each

[27] *Id.* (¶¶ 43–45).

[28] Joint Letter Br. – ECF No. 90.

[29] Joint Letter Br. Ex. 1 – ECF No. 90-1 at 1; Joint Letter Br. – ECF No. 90 at 2 (proposing forensic images as an alternative to production of the devices).

[30] Joint Letter Br. Ex 1 – ECF No. 90-1 at 2.

Mobile Device reflecting or regarding any cookies stored on and/or deleted from the device, including the filenames, contents, and creation/modification/deletion dates of each cookie."[31]

2.1 RFP 1: Inspection or Complete Forensic Images of the Plaintiffs' Mobile Devices

Turn argues that the plaintiffs' mobile devices "are at the very heart of this case."[32] Specifically, with respect to the plaintiffs' New York unfair-business-practices claim, Turn argues that the claim "is wholly dependent on allegations about the content of Plaintiffs' phones, including whether Turn placed (and replaced) cookies on the phones, what kind of cookies Turn placed on the phones (if any) and when, whether Plaintiffs regularly deleted cookies and their browsing history from their phones, whether Turn 'circumvented device settings' on the phones, and what information (if any) was gathered from the phones."[33] With respect to the plaintiffs' trespass-to-chattels claim, Turn argues that "the phones are the very 'chattels' that Plaintiffs allege Turn 'trespassed[.]'"[34] Turn argues that "[i]t's hard to imagine a closer connection between plaintiffs' claims and their phones to justify allowing Turn's digital forensics experts to analyze them directly."[35]

The plaintiffs respond that allowing Turn to inspect their devices or producing a complete forensic image would allow Turn to "access to Plaintiffs' entire phones and thus access to their private text messages, emails, contact lists, photographs and web browsing histories unrelated to Turn."[36] The plaintiffs represent that they objected to RFP 1 and invited Turn to make requests for specific information, which prompted Turn to issue a second, more specific set of requests — RFPs 27–35 — for which (aside from RFPs 32 and 33) the plaintiffs have produced responsive

---

[31] *Id.*

[32] Joint Letter Br. – ECF No. 90 at 2.

[33] *Id.* at 3 (citing Compl. – ECF No. 1 at 22 (¶ 81)).

[34] *Id.*

[35] *Id.*

[36] *Id.* at 8.

information.[37] The plaintiffs argue that Turn's request for the full contents of their devices "flies in the face of Rule 26(b)'s relevancy and proportionality requirements."[38]

2.2 RFP 32: Production of the Web Browsing History on the Plaintiffs' Devices

Turn argues that it is entitled to review the plaintiffs' complete browsing history "[(1)] to investigate whether and to what extent Plaintiffs even visited websites that worked with Turn cookies; [(2)] to test Plaintiffs' claim that they regularly deleted their browsing history in order to protect their privacy; and [(3)] to show that it does not constitute personally identifiable information implicating a protected privacy interest in any event."[39] Turn also argues that the plaintiffs alleged that its cookies "transmit[] a user's web-browsing history back to the third party that generated the cookie, thus allowing the third party to glean valuable information about the user and her (presumed) interests" and that it "is entitled to discovery into all evidence that would provide those allegations untrue."[40]

The plaintiffs respond that producing their full web browser history is overbroad, irrelevant, and invasive of their privacy interests.[41] They argue that "people often browse the Internet for private reasons, such as health, dating, finances, and personal interests."[42] In response to Turn's first argument, the plaintiffs state that they are willing to produce all browsing history associated with Turn partner websites, contingent on Turn's identifying its partner websites.[43] In response to Turn's second argument, the plaintiffs state that (1) their web browsing history does not speak to the zombie-cookie scheme they allege, and that (2) in any event, Turn can discover whether the plaintiffs regularly deleted their browsing history by asking for the date ranges of the history on

---

[37] *Id.* at 6. The top of page 6 identifies the two requests to which the plaintiffs objected as RFP 31 (web browsing history) and RFP 32 (cookies), but the rest of the joint letter brief and the exhibit identifies these as RFPs 32 and 33, respectively.

[38] *Id.* at 7.

[39] *Id.* at 5.

[40] *Id.* at 4–5.

[41] *Id.* at 8–9.

[42] *Id.* at 8 (citing Compl. – ECF No. 8–10 (¶¶ 24–29), 15–16 (¶¶ 50–52)).

[43] *Id.*

their devices, without the contents of the history.[44] In response to Turn's third point, the plaintiffs argue that they "need not disclose the contents of every website ever visited in order to allege that Turn's surreptitious tracking of their web browsing violates Plaintiffs' privacy" and that "whether the information Turn catalogued implicates PII [personally identifiable information] is best determined by evaluating the information Turn has or had in its possession."[45] The plaintiffs also argue that "Turn ignores that it obtains web browsing information by establishing relationships with Turn *partner websites*, and using cookies to track users as they visit those websites over time. And yet Turn's request is not limited to browsing history related to Turn's partner websites — it seeks everything."[46]

2.3 RFP 33: Production of Cookies on the Plaintiffs' Devices

Turn argues that it is entitled to review all cookies stored on the plaintiffs' mobile devices "to technically examine what Turn cookies (if any) are on Plaintiffs' devices and compare them to standard browser cookies — including other non-Turn cookies that Plaintiffs permitted on their devices."[47] Turn argues that "if Plaintiffs have numerous cookies on their devices over a wide range of installation dates, that information would prove their claim [that they regularly deleted cookies] to be false."[48] Turn also argues that "if the devices have cookies dated *after* the complaint, it suggests a failure to preserve key evidence in its original condition."[49]

The plaintiffs respond that their cookies implicate the same privacy interests as their web browsing history.[50] The plaintiffs state that they are willing to produce cookie data related to any

---

[44] *Id.* at 9.

[45] *Id.*

[46] *Id.* (emphasis in original).

[47] *Id.* at 4.

[48] *Id.* at 5.

[49] *Id.*

[50] *Id.* at 9.

Turn partner website, to identify the date fields (but not the contents) of all other cookies, and to meet and confer to consider requests for specific cookies.[51]

ANALYSIS

1. Inspection or Complete Forensic Images of the Plaintiffs' Mobile Devices

The undersigned denies Turn's request to require the plaintiffs to produce their mobile devices for Turn's inspection or, in the alternative, to produce complete forensic images of their mobile devices. Federal Rule of Civil Procedure 26(b)(1) limits discovery to matters that are (1) "relevant to any party's claim or defense" and (2) "proportional to the needs of the case[.]" Turn's request to inspect the plaintiffs' mobile devices or for complete forensic images call for information that is not relevant and is disproportional to the needs of the case.

With respect to relevance, as the plaintiffs correctly point out (and as Turn does not address), Turn's request to directly inspect the plaintiffs' mobile devices or for complete forensic images of the devices threatens to sweep in documents and information that are not relevant to the issues in this case, such as the plaintiffs' private text messages, emails, contact lists, and photographs. Just as a hypothetical request from the plaintiffs for Turn to allow them to directly inspect its emails servers (or produce complete forensic image of its servers) would likely sweep in numerous emails that are not relevant to this action, Turn's request for the plaintiffs to allow it to directly inspect their mobile devices (or produce complete forensic images of their devices) would likely sweep in numerous irrelevant documents as well. *See John B. v. Goetz*, 531 F.3d 448, 457–58 (6th Cir. 2008) (noting that "imaging of these computers and devices will result in the duplication of confidential and private information unrelated to the [] litigation"); *Salazar v. Bocanegra*, No. 12cv0053 MV/LAM, 2012 WL 12893938, at *2 (D.N.M. July 27, 2012) (noting that forensic images, due to their broad nature, may include information irrelevant to the parties' claims or defenses); *Sony BMG Music Entm't v. Arellanes*, No. 4:05-CV-328, 2006 WL 8201075, at *1

[51] *Id.*

(E.D. Tex. Oct. 27, 2006) (finding meritorious responding party's argument that a full forensic image of her computer hard drive would sweep in irrelevant documents).[52]

With respect to proportionality, Turn's request for the plaintiffs to allow it to inspect their mobile devices (or produce complete forensic images of their devices) is disproportional to the needs of the case. While questions of proportionality often arise in the context of disputes about the expense of discovery,[53] proportionality is not limited to such financial considerations. Courts and commentators have recognized that privacy interests can be a consideration in evaluating proportionality, particularly in the context of a request to inspect personal electronic devices. *Tingle v. Hebert*, No. 15-626-JWD-EWD, 2018 WL 1726667, at *7–8 (M.D. La. Apr. 10, 2018) (finding that "Defendants have also made no showing that the requested forensic examination of Plaintiff's personal cell phone and personal email accounts are proportional to the needs of this case" and holding that "'[t]he utility of permitting a forensic examination of personal cell phones must be weighed against inherent privacy concerns'") (quoting *John Crane Grp. Corp. v. Energy Devices of Tex., Inc.*, No. 6:14-CV-178, 2015 WL 11112540, at *2 (E.D. Tex. Oct. 30, 2015)); *Crabtree v. Angie's List, Inc.*, No. 1:16-cv-00877-SEB-MJD, 2017 WL 413242, at *3 (S.D. Ind. Jan. 31, 2017) (denying request to forensically examine plaintiff's personal cell phones and holding that the forensic examination "is not proportional to the needs of the case because any benefit the data might provide is outweighed by Plaintiffs' significant privacy and confidentiality interests"); *Hespe v. City of Chicago*, No. 13 C 7998, at *3 (N.D. Ill. Dec. 15, 2016) (affirming order denying request to inspect plaintiff's personal computer and cell phone because, among other things, inspection "is not 'proportional to the needs of this case' because any benefit the inspection might provide is 'outweighed by plaintiff's privacy and confidentiality interests'"); *Areizaga v. ADW Corp.*, No. 3:14-cv-2899-B, 2016 WL 9526396, at *3 (N.D. Tex. Aug. 1, 2016)

[52] Turn's request might sweep in privileged documents as well, such as emails the plaintiffs might have sent their attorneys that may be stored in email applications on their mobile devices. *Cf. Sony BMG*, 2006 WL 8201075, at *1.

[53] Rule 26(b)(1) expressly provides that "whether the burden or expense of the proposed discovery outweighs its likely benefit" is a consideration in evaluating proportionality.

(denying request to inspect plaintiff's personal computer, smart phone, and other electronic devices because the request "is not proportional to the needs of the case at this time, when weighing [defendant]'s explanation and showing as to the information that it believes might be obtainable and might be relevant against the significant privacy and confidentiality concerns implicated by [defendant]'s request"); *In re Anthem, Inc. Data Breach Litig.*, No. 15-md-02617 LHK (NC), 2016 WL 11505231, at *1–2 (N.D. Cal. Apr. 8, 2016) (denying request to inspect or forensically image plaintiffs' computers, tablets, and smartphones as "invad[ing] plaintiffs' privacy interests" and "disproportional to the needs of the case"); Agnieszka A. McPeak, *Social Media, Smartphones, and Proportional Privacy in Civil Discovery*, 64 U. Kan. L. Rev. 235, 288–91 (2015) (arguing that courts should consider privacy burdens in evaluating proportionality under Rule 26(b)(1)); *see John B.*, 531 F.3d at 460 (issuing writ of mandamus to set aside orders for forensic imaging of state-owned and privately-owned employee computers because, among other things, "[t]he district court's compelled forensic imaging orders here fail to account properly for the significant privacy and confidentiality concerns present in this case"); *see also Johnson v. Nyack Hosp.*, 169 F.R.D. 550, 562 (S.D.N.Y. 1996) (holding that Rule 26 allows courts to limit discovery on account of burden, including "where the burden is not measured in the time or expense required to respond to requested discovery, but lies instead in the adverse consequences of the disclosure of sensitive, albeit unprivileged, material," and that courts should consider "the burdens imposed on the [responding parties]' privacy and other interests").

As the Supreme Court has recognized, "[m]odern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'" *Riley v. California*, 134 S. Ct. 2473, 2494–95 (2014) (citation omitted). As the Court observed:

> Even the most basic phones that sell for less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on. . . .
>
> . . . .
>
> . . . . [I]t is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives — from the mundane to the intimate. . . .

> . . . . An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns — perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building. . . .
>
> Mobile application software on a cell phone, or "apps," offer a range of tools for managing detailed information about all aspects of a person's life. There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life. There are popular apps for buying or selling just about anything, and the records of such transactions may be accessible on the phone indefinitely. There are over a million apps available in each of the two major app stores; the phrase "there's an app for that" is now part of the popular lexicon. The average smart phone user has installed 33 apps, which together can form a revealing montage of the user's life.

Id. at 2489–90 (citations omitted); *accord* McPeak, 64 U. Kan. L. Rev. at 244–45 (discussing how a smartphone can contain information about its owner and her emails, text messages, phone calls, calendars, social-media accounts, photographs, videos, what books she reads, what music she listens to, where she goes, when she sleeps, what she buys, and whom she dates — "[q]uite simply, her [smartp]hone is a portal to a complete, intimate portrait of her entire life"). While *Riley* was a criminal case, courts have applied its observations about the privacy concerns implicated by modern cell phones in the context of civil discovery as well. *See Bakhit v. Safety Mktg., Inc.*, No. 3:13CV1049 (JCH), 2014 WL 2916490, at *3 (D. Conn. June 26, 2014) (citing *Riley* in denying civil-discovery request to inspect personal cell phones).

Turn cites no authorities to support its request that the plaintiffs allow it to directly inspect their mobile devices (or produce complete forensic images of their devices). Turn cites to several cases where courts have ordered a party responding to a discovery request to forensically image its devices — in situations where there was a "sufficient nexus" between the party's devices and the claims or defenses at issue.[54] But forensic imaging itself is not the issue here. The plaintiffs

[54] Joint Letter Br. – ECF No. 90 at 3 (citing cases).

represent that they have already forensically imaged their devices and are producing information from those images.[55] What Turn raises is the separate issue of its being allowed to directly *access* its opponents' devices or forensic images. None of the cases it cites supports that proposition.

Turn's first case, *Calyon v. Mizuho Securities USA, Inc.*, No. 07CIV02241RODF, 2007 WL 1468889 (S.D.N.Y. May 18, 2007), undercuts its request for direct access to the plaintiffs' devices or forensic images. That case, like this one, involved a discovery request for the responding parties (there, the defendants) to produce forensic images of their personal devices. *Id.* at *1. There, as here, the responding parties created forensic images of their devices and offered to search the images (or to have a neutral third-party expert search the images) and produce responsive information. *Id.* at *2. There, as here, the requesting party demanded that it be allowed to directly inspect the entirety of the responding parties' forensic images. *Id.* at *1 ("At bottom, [the requesting party] maintains that only *its* expert — as opposed to the [responding parties]' expert or an independent third-party expert — would possess the requisite incentive to search exhaustively for evidence, and that only [its] expert would be able to confer with [its] counsel on an on-going basis to refine search methods.") (emphasis in original). The court denied the requesting party's request, finding that the requesting party had not made a showing as to why it would be entitled to such "extraordinary" access. *Id.* at *5. Turn's other cases likewise do not support its position. In each of them, the responding party or a neutral third-party expert accessed and produced information from the responding party's forensic images. In none of them did the requesting party directly access its opponent's devices or forensic images. *Cf. Lifetouch Nat'l Sch. Studios, Inc. v. Moss-Williams*, No. C10-05297 RMW (HRL), 2013 WL 11235928, at *2 (N.D. Cal. Oct. 15, 2013) (adopting parties' stipulated protocol that a neutral third-party forensic expert would image computers and produce responsive information therefrom to the parties and that "[n]either [the requesting party]'s personnel nor counsel will ever inspect or otherwise handle [the responding

[55] *Id.* at 7 ("Most importantly, Plaintiffs have already forensically imaged the devices and are producing the categories of information requested, subject to the remaining dispute over web browsing history and cookies, outlined below.").

party]'s computers") (citing Stipulated Protective Protocol for Inspection of the Computers, *Lifetouch Nat'l Sch. Studios Inc. v. Moss-Williams*, No. C10-05297 RMW (HRL) (N.D. Cal. filed July 9, 2012), ECF No. 78 at 4–6); *Genworth Fin. Wealth Mgmt., Inc. v. McMullan*, 267 F.R.D. 443, 449 (D. Conn. 2010) (ordering a third-party forensic expert to image the responding party's devices and provide recovered data to the responding party, which would review data for responsiveness and privilege before producing data to requesting party); *see also Sony BMG*, 2006 WL 8201075, at *1 (denying a party's request to directly inspect the forensic image of its opponent's hard drive in lieu of a neutral third-party expert's doing so).[56]

The parties appear to have in place a protocol for producing information from the plaintiffs' devices or forensic images. Turn has issued nine RFPs (RFPs 27–35) for specific information from the plaintiffs' devices.[57] The plaintiffs represent (and Turn does not deny) that they have produced information from their devices responsive to all of these requests (other than with respect to RFPs 32 and 33 regarding the browsing-history and cookie disputes the parties raise in their joint letter brief, which the undersigned addresses below).[58] Given this, and in light of the fact that the plaintiffs' devices likely contain information not relevant to this case, may contain privileged information, and implicate significant privacy concerns, Turn's request for the plaintiffs to allow it to directly inspect their devices (or produce complete forensic images of their devices) is not relevant or proportional to the needs of this case.

2. Full Web Browsing History and Cookies

The plaintiffs have produced or have offered to produce (1) their web browsing history and cookies associated with Turn partner websites (contingent on Turn's identifying such sites) and

[56] Turn also cites *Austin v. Foodliner, Inc.*, No. 16-cv-07185-HSG (DMR), 2018 WL 1168694 (N.D. Cal. Mar. 6, 2018), to argue that the protective order in this case "is more than sufficient to protect Plaintiffs' privacy concerns." Joint Letter Br. – ECF No. 90 at 5. But the information at issue in *Austin* was just phone-number contact information, and the court there specifically distinguished such contact information from "the disclosure of medical or financial information" or information that "implicates special privacy concerns or threatens 'undue intrusion into one's personal life.'" *Austin*, 2018 WL 1168694, at *2 (citation omitted).

[57] Joint Letter Br. – ECF No. 90 at 6.

[58] *Id.*

(2) the date fields (but not the content) of all other cookies on their mobile devices.[59] The plaintiffs also represent that they offered to meet and confer with Turn to consider requests for specific cookies.[60] The undersigned finds the plaintiffs' position and proposals to be reasonable and proportional, with a slight modification — the plaintiffs should produce the dates (but not the content) of the entries in their browsing history (as they are doing for their cookies).

The undersigned denies Turn's request to require the plaintiffs to produce their full web browsing history and cookie data. As discussed above, requiring the plaintiffs to produce their full browsing history presents significant privacy concerns. *See Riley*, 134 S. Ct. at 2490 ("An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns — perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD."). Cookies, which the plaintiffs assert (and Turn does not deny) are closely associated with websites,[61] raise similar privacy concerns. Turn has not shown that its request for the plaintiffs' full browsing history and cookies as they relate to websites other than Turn partner websites is relevant or proportional to the needs of this case.

Turn claims that it needs to examine what Turn cookies are on the plaintiffs' devices,[62] but the plaintiffs have agreed to produce those cookies, so there is no dispute there. Turn claims it needs web browsing history to determine whether the plaintiffs visited websites that worked with Turn cookies in the first place,[63] but the plaintiffs have agreed to produce their browsing history and cookies for those sites, so again there is no dispute there. Turn claims it needs to compare its

---

[59] *Id.* at 8–9 ("Plaintiffs are amenable — just as they were with regard to cookies — to produce all browsing history associated with Turn partner websites, contingent on Turn's identifying its partner websites. . . . Plaintiffs produced cookie data associated with the turn.com domain, and offered to produce cookie data related to any Turn partner websites. Additionally, Plaintiffs identified the date fields (but not their content) for all other cookies on Plaintiffs' devices (regardless of their association with Turn). . . . Plaintiffs offered in meet and confer to consider requests for specific cookies[.]").

[60] *Id.* at 9.

[61] *Id.* at 9.

[62] *Id.* at 4.

[63] *Id.* at 5.

cookies to standard browser cookies,[64] but it does not need all of the cookies on the plaintiffs' devices to run that comparison. Turn claims that it needs to determine whether the plaintiffs regularly deleted their cookies or browsing histories as they allege,[65] but it can do so through the date fields of the plaintiffs' cookies and browsing histories and does not need the full content of the cookies and histories to do so. Turn claims that the plaintiffs argued that Turn's cookies transmit a user's web-browsing history back to Turn,[66] but Turn has not shown why it needs the plaintiffs' full browsing history to determine what information was or was not transmitted back to Turn (information that is presumably within Turn's possession, custody, or control). Given all this, and in light of the significant privacy concerns present here, Turn has not shown that its request for plaintiffs' full browsing history or cookies is relevant or proportional to the needs of this case.

* * *

As another court in this district noted in the context of a data-breach case, "[t]here is an Orwellian irony to the proposition that in order to get relief for a theft of one's personal information, a person has to disclose even more personal information, including an inspection of all his or her devices that connect to the internet. If the Court were to grant [that] request, it would further invade plaintiffs' privacy interests and deter current and future data theft victims from pursuing relief." *In re Anthem Data Breach*, 2016 WL 11505231, at *1. The same holds true here. There is an Orwellian irony to the proposition that in order to get relief for a company's alleged surreptitious monitoring of users' mobile device and web activity, a person has to allow the company unfettered access to inspect his mobile device or his web browsing history. Allowing this discovery would further invade the plaintiffs' privacy interests and may deter current and future plaintiffs from pursuing similar relief. *Cf. Rivera v. NIBCO, Inc.*, 364 F.3d 1057, 1065 (9th Cir. 2004) (affirming district court's refusal to allow discovery into certain private information of plaintiffs in a Title VII employment case because, among other things, "[t]he chilling effect such

[64] *Id.* at 4.

[65] *Id.* at 4–5.

[66] *Id.* at 4.

discovery could have on the bringing of civil rights actions unacceptably burdens the public interest").

The undersigned does not mean to imply that there could never be an instance where a request to directly inspect a litigant's electronic devices or forensic images, or a request that a litigant produce his complete web browsing history or cookies, would be relevant and proportional. There may be situations where such a request would be proper, and this order is without prejudice to Turn's renewing its request should such a situation arise. But that situation has not presented itself here. Turn's request for the plaintiffs to allow it to directly inspect their mobile devices (or produce complete forensic images of their devices) and for the plaintiffs to produce their complete browsing history and cookies, is denied.

CONCLUSION

The court adopts the plaintiffs' proposals, with the slight modification that the plaintiffs should also produce the dates of the entries in their browsing history.

Going forward, if any other discovery disputes arise, the parties must comply with the dispute procedures in the undersigned's standing order (attached). The procedures in it require, among other things, that if a meet and confer by other means does not resolve the parties' dispute, lead counsel for the parties must meet and confer in person (if counsel are local) and then submit a joint letter brief with information about any unresolved disputes. The letter brief must be filed under the Civil Events category of "Motions and Related Filings > Motions – General > Discovery Letter Brief." After reviewing the joint letter brief, the court will evaluate whether further proceedings are necessary, including any further briefing or argument.

IT IS SO ORDERED.

Dated: October 22, 2018

LAUREL BEELER
United States Magistrate Judge