In Re: Apple Inc. Device Performance Litigation

Case No. 5:18-md-02827-EJD

United States District Court, N.D. California, San Jose Division

Signed 08/22/2019

ORDER DENYING MOTION TO MODIFY SPECIAL DISCOVERY MASTER ORDER NO. 9

Re: Dkt. No. 359

EDWARD J. DAVILA, United States District Judge

*1 After briefing and oral argument by the parties, the Special Discovery Master entered Special Discovery Master Order No. 9 authorizing the forensic imaging of the devices belonging to 10 of the more than 90 named Plaintiffs in order to allow Apple's outside experts to performance-test the devices. Dkt. No. 354 (the "Order"). The Special Discovery Master also ordered the parties to negotiate on a protocol governing the imaging and testing of the devices. *Id.* at 27. The parties submitted a draft protocol for the Special Discovery Master's review and approval on August 5. Dkt. No. 370-2. Plaintiffs maintained their objections. The Special Discovery Master entered the protocol on August 12. Dkt. No. 378 (the "Protocol"). Plaintiffs now move the court to modify the Order, arguing that the Special Discovery Master made erroneous factual findings and reached incorrect legal conclusions. Plaintiffs seek to modify the Order so that Apple's discovery of the devices is limited to the extraction of "limited diagnostic data" instead of full forensic imaging. The motion is suitable for resolution without oral argument. Civil L. R. 7-1(b). The court denies Plaintiffs' motion.

The Order addressed the procedural and factual background, and the basic legal framework and standards for discovery under the Federal Rules of Civil Procedure. To the extent those issues are not in dispute, the Court does not recount them here. Plaintiffs' basic argument is as follows: Personal devices, like those at issue here, are afforded special privacy protections under the law. Apple therefore had to demonstrate a compelling need or interest to justify the forensic imaging. The Special Discovery Master should have conducted a balancing test between that compelling interest and the intrusion into Plaintiffs' privacy posed by the imaging. But the Special Discovery Master failed to do so when she "deferr[ed] the basic question of scientific reliability to trial." Mot. at 3, 7-10. In their Reply, Plaintiffs emphasize that this balancing test also required the Special Discovery Master to evaluate any available alternatives to the imaging. Plaintiffs largely base their arguments on the 2017 California Supreme Court case *Williams v. Superior Court*, which addressed the interplay between privacy rights and discovery. 3 Cal. 5th 531 (2017).

In *Williams*, the court reiterated its framework for assessing potential invasions of privacy. First, "[t]he party asserting a privacy right must establish a legally protected privacy interest, an objectively reasonable expectation of privacy in the given circumstances, and a threatened intrusion that is serious." *Id.* at 552. "The party seeking information may raise in response whatever legitimate and important countervailing interests disclosure serves." *Id.* Where the "threatened invasion of privacy [is] extremely grave," then "only a compelling countervailing interest and an absence of alternatives will suffice to justify the intrusion." *Id.* at 557. "What suffices to justify an invasion will ... vary according to the context." *Id.* Then, "the party seeking protection may identify feasible alternatives that serve the same interests or protective measures that would diminish the loss of privacy." *Id.* at 552. Finally, the "court must then balance these competing considerations." *Id.*

*2 The court finds that Plaintiffs have a legally protected privacy interest in their devices, that their expectation of privacy in their phones is reasonable, and that the threatened invasion is serious. As they argue, personal devicesare afforded special privacy protections. *See Riley v. California*, 573 U.S. 373 (2014); *Henson v. Turn, Inc.*, 2018 WL 5281629 (N.D. Cal. Oct. 22, 2018). *Riley* was a criminal case where the Supreme Court held that "a warrant is generally required before such a search [of a cell phone], even when a cell phone is seized incident to arrest." *Riley*, 573 U.S. at 401. The Court reasoned that "[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.' " *Id.* at 403. "[C]ourts have applied [*Riley*'s] observations about the privacy concerns implicated by modern cell phones [to] the context of civil discovery." *Henson*, 2018 WL 5281629, at *6.

Plaintiffs' concerns over their privacy rights are understandable; they are being asked to surrender their devices and passwords to strangers. Even so, the invasion is not as great as in the *Henson* case. There, the defendant sought to directly examine the phones at issue. Here, the protections of the Protocol lessen the intrusion to Plaintiffs' privacy. Under the Protocol, the forensic imaging will be completed by a neutral, third-party computer forensics vendor, Lighthouse Global ("Lighthouse"). Protocol 1. Lighthouse will disclose the names of everyone who examines or handles Plaintiffs' devices or information and will execute the Stipulated Protective Order entered in this case (Dkt. No. 224). Protocol 2, 3. The devices, their contents, and their passwords will be designated as Highly Confidential – Attorneys' Eyes Only. *Id.* 3, 6. But even then, the forensic copies of the devices will not be provided to counsel, but only to the outside experts. *Id.* 18, 20, 22. The outside experts will only provide counsel with their analyses and the data underlying their analyses. *Id.* To the extent possible, the experts will redact the contents, authors, recipients, and subject-matter of the underlying data (and any associated metadata) or replace them with summary descriptions before providing the underlying data to Apple's counsel. *Id.* If such redactions are not feasible, then Apple will notify the Special Discovery Master who will determine whether to permit the disclosure, not permit the disclosure, or modify the disclosure after hearing from the parties and their experts. *Id.* The experts will not provide irrelevant information such as electronic communications—*e.g.*, text messages or email—photos, audio recordings, video, contacts, location information, medical or financial information, stand-alone documents, cookies, security tokens, IP addresses, or any information that would allow access to user-protected websites or applications. *Id.* The experts will not disclose web-browsing or application-use histories unless such information is identified in the report. *Id.* And if the experts do identify webpages or applications in their report, to the extent possible, they will not list the domain name, or specific webpages. *Id.* Again, if these redactions are not possible, then the Special Discovery Master will consider the redactions after hearing from the parties and their experts. *Id.*While the forensic imaging of 10 of Plaintiffs' devices is a significant invasion into their privacy, the Protocol and Stipulated Protective Order provide robust protections that lessen the invasion as compared to *Henson*.

Next, the court concludes that Apple has a compelling need to obtain this discovery. Most important to this court's consideration is that Plaintiffs are not passive third parties or defendants sued by the party seeking the invasion.

Rather, Plaintiffs actively put their devices at issue when they chose to sue Apple over Apple's alleged intrusion and trespass to the devices through Apple's software updates. It is well-established that a plaintiff cannot bring suit and then limit the defendant's discovery that is targeted at the subject matter of the plaintiff's claims. *See, e.g.*, *Britt v. Superior Court*, 20 Cal. 3d 844, 858 (1978) ("In a number of contexts in which evidentiary privileges generally provide a cloak of confidentiality, exceptions to such privileges have been recognized as to information that relates to an issue which has been posited by the party claiming the privilege's protection."); *Doe v. A. J. Boggs & Co.,* 2019 WL 1517567, at *6 (E.D. Cal. Apr. 8, 2019) ("When evidence is particularly important to a claim or defense, a party's right to discovery of that evidence is more likely to outweigh competing privacy claims."); *Starr v. Lash*, 2017 WL 1400114, at *2 (S.D. Cal. Apr. 19, 2017) ("When evidence is particularly important to a claim or defense, a party's right to discovery of that evidence is more likely to outweigh competing privacy claims."); *Verma v. Am. Express*, 2009 WL 1468720, at *1 (N.D. Cal. May 26, 2009) ("A plaintiff's right to privacy under California and federal law similarly must be balanced against the right of civil litigants to discover relevant facts."); *cf. Memry Corp. v. Ky. Oil Tech., N.V.*, 2007 WL 832937, at *3 (N.D. Cal. Mar. 19, 2007) (denying inspection of computers because the contents of the computers was not "intricately related to the very basis of the lawsuit.").

*3 As discussed above, the privacy concerns attached to personal devices and computers often make courts wary of allowing the forensic imaging of such devices. But courts have ordered such imaging or inspection when those computers and devices were closely connected with the claims and/or defenses in the litigation.

In *Herskowitz/Juel v. Apple Inc.*, the plaintiffs alleged, in part, that Apple prevented consumers from accessing, storing, transferring, or managing purchased products on their devices. Nos. 12-2131-LHK, 12-3124-LHK (N.D. Cal.). Judge Koh ordered the plaintiffs to make their computers and devices available for inspection by the defendant's experts. *Herskowitz/Juel v. Apple Inc.*, Nos. 12-2131-LHK, 12-3124-LHK, Dkt. Nos. 98, 66 (N.D. Cal. Feb. 12, 2014). In *Brocade Communications Systems, Inc. v. A10 Networks, Inc.*, Judge Koh ordered the forensic inspection of a hard drive where to "test[ ] the veracity" of a party's claims. 2012 WL 70428, at *2 (N.D. Cal. Jan. 9, 2012). In *Weatherford U.S., LP v. Innis*, a trade secret case, the court found a

"nexus between [the plaintiff's] claims and its need for images of the defendants' computers." 2011 WL 2174045, at *4 (D.N.D. June 2, 2011). In *Capitol Records, Inc. v. Alaujan*, the district judge found there was a "sufficiently close connection between [the defendant's] Gateway computer ... and the claims in this lawsuit." 2009 WL 1292977, at *2 (D. Mass. May 6, 2009).

Plaintiffs argue that Apple cannot show a compelling interest because the testing sought is neither scientifically reliable, admissible, nor "necessary." Mot. at 3; Reply at 1. They argue that the forensic imaging would "violat[e] Plaintiffs' privacy with no gain" to Apple. Mot. at 3. Plaintiffs overreach. The compelling interest standard may be a higher bar than relevance and proportionality, but it does not require Apple to make a threshold showing that the sought-after information will be admissible, scientifically reliable, and "necessary." While the cases cited by Plaintiffs recognize and apply a heightened standard, none required the party seeking the discovery to first show that the sought-after information meets Plaintiffs' criteria. *Lawrence v. Hoban Mgmt., Inc.*, 305 F.R.D. 589, 593 (S.D. Cal.), *on reconsideration in part*, 103 F. Supp. 3d 1216 (S.D. Cal. 2015) (denying discovery where the plaintiffs failed to show "any" need for the third-party discovery); *Cefalu v. Holder*, 1013 WL 4102160, at *1 (N.D. Cal. Aug. 12, 2013) (denying forensic imaging of the plaintiff's hard drives for failure to show "good cause" and the plaintiff's counsel could ensure that any responsive material on the hard drives would be produced); *Artis v. Deere & Co.*, 276 F.R.D. 348, 353 (N.D. Cal. 2011) (allowing discovery after balancing the privacy interests of the relevant third parties against the plaintiffs' interest in the discovery); *Britt*, 20 Cal. 3d at 858 (finding that the requested discovery was not warranted because it "reach[ed] far beyond the privacy interests of the plaintiffs ... and directly impinge[d] on the constitutional rights of numerous individuals who have taken no action whatsoever with respect to the underlying lawsuit."). Apple is not required to show that the sought-after evidence is admissible, scientifically reliable, or "necessary" before obtaining the discovery at issue.

The court finds that Apple has a compelling interest in the sought-after performance testing of Plaintiffs' devices. The devices' performance is integral to Plaintiffs' claims. They allege that Apple's software updates unjustly harmed the performance of their devices. *See, e.g.*, SAC 402-405. Apple is entitled to defend itself against these allegations by testing whether the performance of the devices was, in fact, harmed. Later, Plaintiffs may challenge whether that testing is admissible, scientifically reliable, or "necessary" for Apple's defenses through *in limine, Daubert*, and other motions.

Next, Plaintiffs argue that the Special Discovery Master erred by not considering the availability of alternatives to the full forensic imaging. Under *Williams*, it is Plaintiffs, as "the party seeking protection," that "may identify feasible alternatives." 3 Cal. 5th at 552. They maintain that the extraction of limited diagnostic data should be sufficient for Apple. The court is not persuaded.

A full forensic image of the phones will allow Apple's experts to test the performance of the devices as Plaintiffs actually use them—to evaluate their performance subject to demands and impacts caused by each device's particular configuration, applications, usage history, and data. Martin Rep. 6-7, 11-15. Plaintiffs have not shown that their proposal to allow the extraction of limited diagnostic data is a feasible alternative. They suggest that such diagnostic data would include whether and when a Plaintiff downloaded the software updates, but it is not at all clear what other data other Plaintiffs propose providing. Plaintiffs' references to the testimony of Apple witnesses do not move the needle. The witnesses testified that Apple may already have data that can be used to "infer" whether a device's performance was impacted. But, the undefined diagnostic information and the data that Apple may already possess are simply not adequate alternatives to actually testing whether a device's performance suffered as to, *e.g.*, application launch times, scrolling speed, memory usage, or animation performance. *See* Martin Rep. 6.

*4 The court finds the forensic imaging presents a serious invasion of Plaintiffs' significant and protectable privacy interest in their devices. That invasion is lessened, though, by the robust protections of the Protocol and the Stipulated Protected Order.

Apple's interest in performance testing the forensic images outweighs Plaintiff's privacy interest because Plaintiffs put the performance of the devices at the center of the lawsuit. The court further finds that Plaintiffs have not presented a feasible alternative that will satisfy Apple's interest in the performance testing. The motion is denied.

IT IS SO ORDERED.

End of Document.