New York Law Journal
Technology Today
WWW.NYLJ.COM
An ALM Publication
VOLUME 262—NO. 65
TUESDAY, OCTOBER 1, 2019

FEDERAL E-DISCOVERY

Court Allows Forensic Imaging Of Personal Devices


By **Christopher Boehning** And **Daniel J. Toal**

Federal Rule of Civil Procedure 26(b)(1) allows parties broad discovery of "any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case … . " However, when discovery includes protected personal information, courts may find themselves weighing the allowable scope of discovery against the personal privacy interests of individuals.

Late last year, we wrote about a case from the Northern District of California where the magistrate judge, balancing privacy and discovery, rejected a request to produce personal devices in their entirety. Just recently, however, a district judge from the same district conducted a similar analysis, but allowed the forensic imaging of personal devices after finding that a compelling need for discovery outweighed privacy interests. This recent case demonstrates the evolving nature of the balancing process between these competing interests and can serve as a helpful guide to judges who will have to navigate the issue in the future, especially as data privacy laws expand around the world and within the United States.

'In re: Apple'

In the putative class action *In re: Apple Inc. Device Performance Litigation*, 2019 WL 3973752 (N.D. Cal. Aug. 22, 2019), the plaintiffs alleged that Apple's software updates harmed the performance of their personal Apple devices. On July 9, 2019, the Special Discovery Master for the matter granted Apple's request to conduct full forensic imaging of the devices of ten of the over ninety named plaintiffs. The corresponding Order required the parties to negotiate a "protocol governing the imaging and testing of the devices." Id. at 1.

This recent case demonstrates the evolving nature of the balancing process between these competing interests and can serve as a helpful guide to judges who will have to navigate the issue in the future, especially as data privacy laws expand around the world and within the United States.

The plaintiffs moved for reconsideration of the Special Discovery Master's Order, "seek[ing] 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." Id. The plaintiffs argued that, as ordered, the forensic imaging of their entire personal devices would represent an unjustified intrusion into their privacy. Given that personal devices have privacy protections under the law, the plaintiffs contended that Apple should have first established why its compelling interest in the full devices outweighed their privacy interests and, then, the Special Discovery Master, in turn, should have weighed these competing interests. Id.


SHUTTERSTOCK

Here, the court agreed with the plaintiffs' concerns over their privacy, finding "that Plaintiffs have a legally protected privacy interest in their devices, that their expectation of privacy in their

CHRISTOPHER BOEHNING *and* DANIEL J. TOAL *are litigation partners at Paul, Weiss, Rifkind, Wharton & Garrison. Ross M. Gotler, e-discovery counsel,* LIDIA M. KEKIS, *e-discovery attorney, and* ALAN D. WILBUR, *senior e-discovery project manager, assisted in the preparation of this article.*

phones is reasonable, and that the threatened invasion is serious. As they argue, personal devices are afforded special privacy protection." Id., citing *Henson v. Turn*, 2018 WL 5281629 (N.D. Cal. Oct. 22, 2018). In *Henson*, as we wrote last year, a magistrate judge denied requests by the defendants to inspect personal devices of the plaintiffs and to collect web browsing history and cookies from the devices on the basis that the data sought was neither relevant nor proportional to the needs of the case.

The court found, though, that compared to *Henson,* the *In re: Apple* plaintiffs were at significantly less risk of having their privacy intruded upon. Here, the Special Discovery Master had approved a "protocol governing the imaging and testing of the devices" that had been negotiated by the parties—while the plaintiffs maintained their objections—and that contained a series of protective measures. In re: Apple, at *1.

Under the protocol, collection and processing were conducted by a "neutral, third-party computer forensics vendor" engaged as experts. Id. at *2. The vendor was to disclose everyone who handled or examined the plaintiffs' devices or information, and each of those people had to individually execute a protective order. The experts were to exclude any "irrelevant information" such as communications, photos, audio, video, contacts, or geolocation and would not disclose irrelevant history of web browsing or application use. Additionally, the devices, their contents, and passwords were all designated under the protective order as "Highly Confidential—Attorneys Eyes Only" and, even then, not provided to counsel for Apple. Rather, the experts at the vendor only were to "provide counsel with their analyses and the data underlying their analyses." Id. Redactions were to be used wherever possible, and if not possible, the evidence would be reviewed in camera prior to divulging it to the defendant. Distinguishing Henson, the court concluded that, "[w]hile 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." Id.

Compelling Interest

Next, the court addressed the plaintiffs' argument that due to the nature of the discovery, to obtain it Apple must have a compelling interest—a higher standard than relevance and proportionality—and that such a compelling interest did not exist. The court noted that "the privacy concerns attached to personal devices and computers often make courts wary of allowing the forensic imaging of such devices" and that the cases cited by the plaintiffs did indeed "recognize and apply a heightened standard." Id. at *3.

'In re: Apple' highlights the natural tension between privacy and discovery and that courts will increasingly be called upon to balance the two as part of defining the permissible scope of discovery.

However, here the devices and their performance were integral to the plaintiffs' claims; thus, the court found that Apple did have a compelling interest in performance testing the devices. The court wrote 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." Id. at *2. Since the plaintiffs alleged that the performance of their devices was harmed by these updates, "Apple is entitled to defend itself against these allegations by testing whether the performance of the devices was, in fact, harmed." Id. at *3.

The plaintiffs additionally argued that the Special Discovery Master had "erred by not considering the availability of alternatives to the full forensic imaging." After noting that the burden is on the party seeking protection to identify feasible alternatives, the court rejected the plaintiffs' suggestion of providing limited diagnostic data and accepted Apple's argument that it had no reasonable substitute to full forensic images for evaluating the devices' performance.

While finding that the "forensic imaging presents a serious invasion of Plaintiffs' significant and protectable privacy interest in their devices," the court found such invasion "lessened, though, by the robust protections of the Protocol and the Stipulated Protected Order." Id. at *4. Weighing this against Apple's interest in obtaining the discovery, the court denied the plaintiffs' motion for reconsideration, stating that "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 … . Plaintiffs have not presented a feasible alternative that will satisfy Apple's interest in the performance testing." Id.

Conclusion

Data privacy laws such as the European Union's General Data Protection Regulation and the California Consumer Privacy Act—set to go into effect in 2020—establish and protect indiv iduals' rights over their personal information. *In re: Apple* highlights the natural tension between privacy and discovery and that courts will increasingly be called upon to balance the two as part of defining the permissible scope of discovery.