New York Law Journal
Technology Today
WWW.NYLJ.COM
An ALM Publication
VOLUME 260—NO. 107
TUESDAY, DECEMBER 4, 2018

FEDERAL E-DISCOVERY

Court Weighs Data Privacy Concerns in Discovery Analysis


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

Data privacy has been the subject of countless headlines this year thanks to a number of high profile data breaches, international data protection laws such as the EU General Data Protection Regulation (GDPR), and domestic developments such as the CLOUD Act and the California Consumer Privacy Act.

In the U.S. discovery context, the impact of the increased focus on data privacy has been less clear. Although parties, practitioners, and judges are more aware of data privacy obligations and the data privacy rights of individuals, the jury has remained out on the question whether that awareness will translate into narrowed discovery. A recent decision from a federal magistrate judge, however, provides support for those who want courts to factor data privacy concerns into their determinations of the permissible scope of discovery.


SHUTTERSTOCK

'Henson v. Turn'

In the data privacy class action *Henson v. Turn*, 2018 WL 5281629 (N.D. Cal. Oct. 22, 2018), two New York residents brought claims against a marketing company for alleged trespass to chattels and for deceptive acts and practices in violation of New York Business Law §349. The action relates to "cookies," described in the decision as lines of software code that "monitor and gather information about a user's website browsing and app use, which includes personal information regarding the user's daily routines. The resulting data is analyzed and used to target advertisements that match the user's profile." Id. at *1. The plaintiffs alleged that the defendant placed onto their mobile devices "zombie cookies," which are "cookies that users either cannot delete or block or that, when users try to delete them, 'respawn' to continue tracking users across the web." Id.

During discovery, the defendant requested that the plaintiffs produce their actual mobile devices, or complete forensic images thereof. The plaintiffs claimed that after objecting to this request and inviting the defendants to make requests for more specific information, the defendants made two additional requests, for all web browsing history and all cookies from these devices. In the instant action, the court ruled on the defendant's demand that it require the plaintiffs to comply with these production requests; the plaintiffs opposed on the grounds that the requests were overbroad and would invade their privacy rights.

Plaintiffs' Mobile Devices

In support of its request for inspection or forensic images of the plaintiffs' mobile devices, the defendant argued

CHRISTOPHER BOEHNING *and* DANIEL J. TOAL *are litigation partners at Paul, Weiss, Rifkind, Wharton & Garrison.* ROSS M. GOTLER, *e-discovery counsel, and* LIDIA M. KEKIS, *e-discovery attorney, assisted in the preparation of this article.*

that the devices themselves "are at the very heart of this case" because they "are the very 'chattels' that Plaintiffs allege [the defendant] trespassed" and their contents directly tie into the unfair business practices claim. Id. at *4. The plaintiffs objected, arguing that the request would provide the defendant with "access to Plaintiffs' entire phones and thus access to their private text messages, emails, contact lists, photographs and web browsing histories unrelated to [the defendant]" and that it "flies in the face of Rule 26(b)'s relevancy and proportionality requirements." Id. Federal Rule of Civil Procedure 26(b)(1) limits the permissible scope of discovery to "any non-privileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering … whether the burden or expense of the proposed discovery outweighs its likely benefit." Fed. R. Civ. P. 26.

Conducting its analysis under this rule, the court first addressed the defendant's request for full access to or forensic images of the plaintiffs' mobile devices. With respect to the question of relevance, the court agreed with the plaintiffs' argument that the request for full access to the devices would also sweep in irrelevant (and private) documents along with potentially privileged communications such as email messages to and from the plaintiffs' attorneys.

Turning next to a proportionality analysis under Rule 26(b)(1), the court noted that "[w]hile questions of proportionality often arise in the context of disputes about the expense of discovery, 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." *Henson,* 2018 WL 5281629 at *5. The court proceeded to cite several cases finding discovery requests to be disproportionate to the needs of the case where the burdens imposed on the responding party's privacy and confidentiality interests outweighed any benefit from inspection of the electronic devices. See id. at *5.

Thus, having determined that "the plaintiffs' devices likely contain information not relevant to this case, may contain privileged information, and implicate significant privacy concerns," id. at *7, the court rejected the defendant's production request for the devices themselves (or forensic images thereof), finding the request neither relevant nor proportional to the needs of the case.

> A recent decision from a federal magistrate judge provides support for those who want courts to factor data privacy concerns into their determinations of the permissible scope of discovery.

Web Browsing History and Cookies

Next, the court considered the defendant's requests for all web browsing history and for all cookies from the plaintiffs' devices. Addressing one by one the defendant's claimed needs for such information, the court, for each, indicated that the need related to an issue no longer in dispute or was achievable with a more narrowly tailored production, as offered by the plaintiffs. For example, the court stated that the defendant "claims that it needs to determine whether the plaintiffs regularly deleted their cookies or browsing histories as they allege, 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." Id. at *8.

Finding, again, that the defendant failed to show how the requests were relevant and proportional to the needs of the case, the court rejected the defendant's requests for full web browsing history and for all cookies and, instead, adopted (with a slight modification) the plaintiffs' alternative proposal to produce more limited information.

Conclusion

As more and more of our actions are online and our devices provide a growing de facto digital record of our lives, data privacy concerns will become increasingly relevant. As *Henson* demonstrates, the classic requirements of the U.S. discovery process may further implicate data privacy issues when non-relevant personal information might be swept into a document collection.

As such, courts and practitioners should have a heightened awareness of these issues and be sure to weigh data privacy concerns as part of considering and determining the permissible scope of discovery. And, courts may be likely to determine, as in *Henson*, that the burdens imposed on a responding party's privacy are significant enough to outweigh any probative value from the information sought. As the magistrate judge in *Henson* pointedly noted, "[t]here 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." Id.