UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

ALBERT AMINOV,

Plaintiff,

v.

BERKSHIRE HATHAWAY GUARD INSURANCE COMPANIES, and AMGUARD INSURANCE COMPANY,

Defendants.

ORDER
21-CV-479-DG-SJB

BULSARA, United States Magistrate Judge:

Defendant AmGuard Insurance Company has moved to compel Plaintiff to produce—for forensic examination—the cell phone that recorded videos produced by Plaintiff. The motion is denied.

"Forensic examinations of computers and cell phones are generally considered a drastic discovery measure because of their intrusive nature." *Stewart v. First Transit, Inc.*, Civ. No. 18-3768, 2019 WL 13027112, at *1 (E.D. Pa. Sept. 3, 2019) (quotations omitted); *see also* Fed. R. Civ. P. 34(a) advisory committee's note to 2006 amendment ("Inspection or testing of certain types of electronically stored information or of a responding party's electronic information system may raise issues of confidentiality or privacy. The addition of testing and sampling to Rule 34(a) with regard to . . . electronically stored information is not meant to create a routine right of direct access to a party's electronic information system, although such access might be justified in some circumstances. Courts should guard against undue intrusiveness resulting from inspecting or testing such systems."). "[E]ven if acceptable as a means to preserve electronic evidence, compelled forensic imaging is not appropriate in all cases, and

courts must consider the significant interests implicated by forensic imaging before ordering such procedures." *John B. v. Goetz*, 531 F.3d 448, 460 (6th Cir. 2008). As such, "in situations where a party can show improper conduct on the part of the responding party, a forensic examination may be appropriate." *Preston v. Cnty. of Macomb*, No. 18-12158, 2021 WL 4820556, at *3 (E.D. Mich. Oct. 15, 2021) (alteration omitted). For example, "[i]t is well-settled that discrepancies or inconsistencies in the responding party's discovery responses may justify a party's request to allow an expert to create and examine a mirror image of a hard drive." *Schreiber v. Friedman*, No. 15-CV-6861, 2017 WL 11508067, at *5 (E.D.N.Y. Aug. 15, 2017) (quotations omitted). "Courts have also ordered computer imaging when there is reason to believe that a litigant has tampered with the computer or hidden relevant materials that are the subject of court orders." *Id.* (collecting cases). But in the end, there must be good cause to order computer imaging, *id.*, or similar forensic examinations, when a party has already produced the electronic information sought and in a native format. Fed. R. Civ. P. 34(b)(E)(iii) ("A party need not produce the same electronically stored information in more than one form."); *e.g.*, *In re Ford Motor Co.*, 345 F.3d 1315, 1317 (11th Cir. 2003) ("[D]irect access might be permissible in certain cases, this case has not been shown to be one of those cases. [A party] . . . is unentitled to this kind of discovery without—at the outset—a factual finding of some non-compliance with discovery rules[.]"); *FCA US LLC v. Bullock*, 329 F.R.D. 563, 568 (E.D. Mich. 2019) ("FCA simply asserts that Bullock has done something dishonest, but offers no evidence that would lead the Court to believe she is secretly withholding information. Bullock has handed over more than 1,300 documents and has stated that these are all of the relevant materials that she has.").

Here there is no such justification. As an initial matter, the motion is based on misplaced and unsupported speculation. AmGuard alleges that there is reason to believe that the metadata for the video was altered. This belief is based on counsel's own analysis using a free online metadata tool: www.metadata2go.com (last visited Mar. 3, 2022). Nothing about the tool used—including its reliability—is asserted. And counsel bases his entire set of assumptions on the less-than-unequivocal statement produced by the website when Plaintiff's videos were analyzed: "Metadata could have been changed or deleted in the past." (Letter Mot. to Compel Discovery dated Feb. 16, 2022, Dkt. No. 19 at 2 (emphasis omitted)). This is hardly the kind of analysis or support that provides a reasonable basis either to conclude that there was alteration of metadata or to warrant forensic examinations. And as explained below, the lack of certainty and ambiguity in the statement makes sense—once one appreciates that this disclaimer is provided by the company for every file it analyzes.

Besides the uncertainty in the Metadata2Go statement, the tool itself is not one designed to show alteration of metadata, but instead one that determines whether metadata exists. According to the website: "Metadata2Go.com is a free online tool that allows you to access the hidden . . . meta data of your files." Its terms of service similarly say: "The Provider provides an infrastructure on metadata2go.com, which should facilitate the User to receive a list of metadata stored in their files." In other words, the website reveals metadata, and therefore—at best—it may have revealed that videos were produced without metadata. Nowhere does the website purport to suggest that the program be used to infer metadata alteration or deletion. And indeed, the absence of metadata cannot actually be inferred. The message that counsel quotes about alteration—that the metadata "could have been changed or deleted"—appears

automatically for *every* file that is uploaded on the website, as a means of liability protection for the company operating the website. The sentence in the disclaimer which follows, and which is not quoted, reflects this. The company says: "[T]he metadata is provided without liability." (The Court used the program on one of its own files, which had no metadata alteration, as an example). In other words, it is not specific to Plaintiff's video. The warning or disclaimer appears for every file analyzed by the website. This is hardly the thing on which one should base a motion to compel. Counsel has layered a series of speculations upon a series of flawed assumptions and misguided understandings of the program. And although counsel spoke to a forensic consultant, his motion did not offer the consultant's opinion about the website, but referred to it only to support the idea that the original phone is necessary for metadata examination. Nor did the consultant opine that Plaintiff's files have missing or altered metadata. (And not in the form of a declaration or other admissible submission, but through summary presentation by counsel.) As for Defendant's other retained expert, his opinion that the videos have different "media created date[s]" is also an unsupported assertion. The expert is a civil and structural engineer, not a computer expert, and he provides nothing other than the conclusory statement about the creation dates of the video. That is, he does not opine that there has been metadata alteration. At the end of the day, Plaintiff has provided native versions of the video; it has some metadata associated therewith. Since there is no evidence of spoilation or alteration, there is no cause to require forensic examination of the cell phone on the speculation that additional metadata may exist or that the original metadata was altered. *Sophia & Chloe, Inc. v. Brighton Collectibles, Inc.*, No. 12cv2472, 2013 WL 5212013, at *2 (S.D. Cal. Sept. 13, 2013) ("[A]bsent more specific, concrete evidence of concealment,

destruction of evidence, or failure to preserve documents and information, plaintiff is not entitled to access defendant's computers to confirm its suspicions.").[1] The motion is denied.

SO ORDERED.

/s/ *Sanket J. Bulsara* 3/3/2022
SANKET J. BULSARA
United States Magistrate Judge

Brooklyn, New York

[1] Defendant served a "Notice to Produce" the cell phone for examination. Even if there were a basis to require the examination, the motion would be denied because the proposed examination of the phone is unlimited, not taken with steps to protect privacy or restrict access to irrelevant information, and does not specify the person or procedures that would be used to conduct the examination.