IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NORTH DAKOTA

Joshua Peterson, Plaintiff, vs. City of Minot, a political subdivision, and Officer Brandon Schmitt, a Minot Police Officer, in his individual capacity Defendants.	)	**ORDER GRANTING IN PART AND DENYING IN PART MOTION TO COMPEL** Case No.1:16-cv-271

Before the court is a motion by defendants to compel discovery from plaintiff's laptop computer. This is the second time a discovery issue with respect to this computer has come before the court.

I. BACKGROUND

During the early morning hours of August 30, 2014, plaintiff, an admitted methamphetamine addict and drug dealer, drove into an area behind several commercial establishments located on the periphery of downtown Minot, North Dakota. Brandon Butler, also an admitted methamphetamine user and purported drug-dealing associate of plaintiff, was a passenger. Plaintiff pulled his vehicle up to the back entrance of Minot Welding Company and proceeded to burglarize the establishment while Butler remained in the vehicle

While in Minot Welding, plaintiff observed a Minot police vehicle pull up across the street from the front side of the building. Recognizing he might be in trouble, plaintiff exited out the back

to where his vehicle was parked. As police officers converged on the area in back of the business establishments, plaintiff pulled his vehicle away in attempted flight. As he was doing so, defendant Schmitt fired five rounds from relatively close range into the side of the vehicle, several of which struck plaintiff and Butler. Plaintiff was seriously injured and rendered a paraplegic. Butler was not so seriously injured.

Following these events, plaintiff was not incarcerated while he recovered from his injuries and underwent some rehabilitation. Later, and after accumulating new charges, he was sentenced to prison and is still serving his sentence.

Plaintiff initiated this action against the City of Minot and Officer Schmitt in his individual capacity, alleging that Schmitt violated his federal constitutional rights by using excessive force. Plaintiff also asserts state law claims of battery and negligence.

During the taking of depositions in this case, defendants became aware that plaintiff had a laptop computer that was then being held by his parents. Prior to that, plaintiff's then spouse, who was separated from plaintiff and has now since divorced him, had possession of the computer for a period of time after plaintiff went to prison, before turning it over to plaintiff's parents. Relevant to what follows, it appears plaintiff used the computer for some period of time following the incident that is the subject of this action and so did plaintiff's ex-spouse while she had possession of it.

After learning of the laptop, defendants sought to inspect the computer—if not outright gain possession of it—by serving a Rule 45 subpoena upon plaintiff's parents directing them to produce the computer at the Minot Police Department. When plaintiff's counsel complained about this in

a letter, defendants' counsel stated in response that they intended to ship the computer to an expert in Minneapolis for examination and that plaintiff's attorneys could have someone in attendance for the examination. Nothing was offered in terms of any limitation upon the extent of the search. Plaintiff then moved to quash the subpoena and defendants moved to enforce it—claiming that they had the right to an unfettered inspection of the computer. In a prior order dated January 8, 2018, the court (1) granted plaintiff's motion to quash the subpoena, and (2) denied defendants' motion to compel enforcement of it. The court, however, did require that plaintiff's counsel take possession of the computer to insure that any information on it was properly preserved. The court then went on to state:

> The court further concludes that defendant does not have the right to go on a fishing expedition to examine the computer for whatever might suit its interest. Consequently, the subpoena to plaintiff's parents will be quashed.
>
> That being said, given the particular circumstances of the case and the fact that we are still a long way prior to trial, the court will allow defendant to make a very targeted request to the plaintiff for discovery of additional information that may be on the computer that is not cumulative of what defendant has already obtained from plaintiff during his deposition. Plaintiff's counsel can then respond accordingly, either by objecting (but not on the basis that discovery has closed) or providing responsive information that is on the computer, if any. Any disputes can be resolved by motion, but only after first following the procedure for informal resolution of the disputes through a phone call to the undersigned as required by our Local Rules.

(Doc. No. 43).

Following the court's order, defendants did make what they styled as a "Request for Discovery of Additional Information From Joshua Peterson's Laptop." The individually numbered requests describe a number of possible locations on the computer for electronic information (*e.g.*, email, social media, file exchange, messaging, photo, and internet browser programs) and then asks

for virtually all files and other information at these locations, including deleted information. The individual requests are as follows:

> REQUEST NO. 1: Please produce any and all Viber history and records, including deleted history, from the subject laptop. *See* attached page 43 of Raquel Peterson's deposition transcript regarding Joshua Peterson's use of Viber on the subject laptop.
>
> REQUEST NO. 2: Please produce any and all messaging or communication applications or programs records from the subject laptop, including deleted or purged items. *See* attached page 44 of Raquel Peterson's deposition transcript regarding Joshua Peterson's use of "other form of communication [on subject laptop] besides his cell phone."
>
> REQUEST NO. 3: Produce all resident email account (*e.g.*, Outlook) records from the subject laptop, including usernames, sent items, received items, subject lines, for and from lines, dates of activity, email content, contacts list, and deleted or purged items. *See* attached page 45 of Raquel Peterson's deposition transcript regarding Joshua Peterson's use of the subject laptop to communicate through email, including after the subject incident.
>
> REQUEST NO. 4: Please produce all third-party web-based email account (e.g. Google, Hotmail, Yahoo) records from the subject laptop, including usernames sent items, received items, subject lines, to and from lines, dates of activity, email content, contact lists, and deleted or purged items. *See* attached page 45 of Raquel Peterson's deposition transcript regarding Joshua Peterson's use of the subject laptop to communicate through email, including after the subject accident, and page 44 of Raquel Peterson's deposition transcript regarding Joshua Peterson's use of at least one "gmail" email account and page 45 of Raquel Peterson's deposition transcript regarding Joshua Peterson's use of the subject laptop to communicate through email, including after the subject incident.
>
> REQUEST NO. 5: Please produce any and all internet history from any browser used on the subject laptop, including deleted or purged history.
>
> REQUEST NO. 6: Please produce any and all photos and/or videos on the subject laptop, including deleted or purged photos and/or videos. *See* attached page 46 of Raquel Peterson's deposition transcript stating that at least one deletion of the subject laptop has occurred since the subject incident.
>
> REQUEST NO. 7: Please produce any and all social media records from the subject laptop, including deleted and/or purged records, contact lists, and friends lists.
>
> REQUEST NO. 8: Please produce all user created files, including deleted files, and the dates they were deleted. *See* attached page 46 of Raquel Peterson's deposition transcript stating that at least one deletion of the subject laptop has occurred since the subject incident.

> REQUEST NO. 9: Please provide any and all records from data destruction programs. or indications of data destruction.
>
> REQUEST NO. 10: Please provide any and all records of transferring of files between the subject laptop and any external electronic device or data storage unit. *See* pp. 223-224 of Joshua Peterson's deposition transcript acknowledging that he has transferred files between the subject laptop and other electronic devices.

(Doc. No. 69-1).

While there are no limitations set forth in the individual requests with respect to subject matter or time, the defendants did state the following in the predicate to the requests:

> **SCOPE OF DOCUMENTS REQUESTED AND TO BE PRODUCED**
>
> "Subject incident" or "incident" is described as the incident occurring on August 30, 2014 when plaintiff Joshua Peterson was in the vicinity of 400 4th Avenue Northeast, at and/or near Minot Welding Company, Minot, ND, as described in the *Complaint and Jury Trial Demanded* (doc. 1) elated July 22, 2016 (hereinafter "Subject Complaint"). For purposes of these requests, the following requests are **limited to responsive documents and/or files, including deleted files, from 30 days prior to the subject incident until 30 days after the subject incident.** "Responsive documents" include any and all forms of documents, files, or electronically stored information ("EST"), including deleted and/or purged documents, related to: methamphetamine possession, use and/or trafficking of methamphetamine, including all references to the same by street names or slang, such as, but not limited to, "meth", "crystal", and "rock"; communications that Joshua Peterson had with witnesses and/or potential witnesses, for purposes of the requests "witnesses and/or potential witnesses" is limited to the following: Megan Owens, Brandon Butler, the persons that Brandon Butler testified that he visited in the early morning hours on August 30, 2014, any other individuals that Joshua Peterson interacted with in relation to methamphetamine trafficking, any other individuals that Joshua Peterson interacted with in relation to the buying or selling of stolen goods, and any communications related to the subject incident."

(Id.) (bolded type in original).

After this demand was made, plaintiff's attorneys took the computer to a local computer store in Minot to assist in responding to the requests without advising defendant's counsel of their intentions. The local computer store conducted an examination of the computer that resulted in

some information being recovered (apparently none of it helpful to defendants) and generated a report of its findings relative to the individual requests as follows:

> *Request No. 1:* No Viber program found on computer. No Viber history or records found on computer. Looked for Viber program - not found. Scanned HD for Viber references - none found. If software was on computer it may have been uninstalled/deleted.
>
> *Request No. 2:* No messaging or communications programs, except email programs, found on computer. Looked for messaging and communications programs - none found. If programs were on computer they may have been uninstalled/deleted.
>
> *Request No. 3:* Found Windows Mail and MS Outlook email programs on computer. Neither program has any local email or email accounts. Windows Mail is currently configured to access a web-based email account. Looked for email programs - found Win Mail and MS Outlook. Looked for local mail repositories - none found. Outlook appears not to have been used. Mail wants to use Microsoft to access web-based email account(s). May be able to use computer to access web email.
>
> Request No. 4: No third-party web-based email found on computer. All email for web-based email accounts is stored on the web. Looked for locally stored email data from web-based programs - none found. Neither Gmail or Yahoo store email on local computer.
>
> *Request No. 5:* Web browsers found - Internet Explorer, Firefox, and Chrome. IE is set to delete history after 20 days. Found browser history for Firefox - exported history to external HD. Scanned HD for web browser history. Copied files found to external HD. Used history viewer program to view browser history and export history in readable format for dates needed to external HD.
>
> *Request No. 6:* Exported pictures to external HD. Scanned HD for all image files for dates needed. Copied all files to external HD. Looked at files - 90% of files are images from program installation/usages. Deleted those files from external HD. Had to restore folders from Windows Recycle Bin to look at files contained. Copied files from needed dates to external HD. Returned files to Recycle Bin.
>
> *Request No. 7:* No social media programs installed on computer. Any social media websites would store on their servers not on local computer. Looked for social media programs - none found. Almost all social media platforms (ie. Facebook) used on computers are accessed through web browsers and keep data on their servers.
>
> *Request No. 8:* Exported documents to external HD. Scanned HD for all document files for dates needed. Copied all files to external HD. Had to restore folders from Windows Recycle Bin to look at files contained. Copied files from needed dates to external HD. Returned files to Recycle Bin.

> *Request No. 9:* No data destruction programs found on computer. Looked for data destruction programs • none found. If programs were on computer they may have been uninstalled/deleted.
>
> *Request No. 10:* Not able to find data. Have no software needed to provide this info.

(Doc. No. 69-3). Plaintiff's counsel then furnished the report to defense counsel along with the recovered electronic data. Plaintiff's counsel also made a formal written response to the individual requests stating that what information that could be retrieved during the proposed 60-day window straddling the shooting incident was turned over and that the requests were in any event variously vague, overbroad, unduly burdensome, not relevant, and/or not reasonably calculated to lead to the discovery of relevant evidence.

Defendants have employed the services of a forensic computer expert who has provided an affidavit stating that the search conducted by the local computer store was inadequate and may have compromised the information that was existing at the time it conducted the search.[1] Defendants in their present motion ask the court to either order complete responses to the requests or, in the

[1] Defendants' counsel subsequently wrote plaintiff's counsel a letter blaming them for purported "significant spoilation" occurring as a result of the attempt to retrieve information made by the local computer store and failing to address defendants' proposal for the computer to be first imaged by plaintiff's counsel and a copy of the image sent to defendant's counsel. Certainly, the better practice would have been for an image to have been made of the computer by the local computer store and for it to have worked from that image. That being said, while the court is going to permit a limited forensic examination, there is not at this point any definitive evidence there was any information relevant *to this case* on the computer. Further, in this court's view, the failure to reach a compromise on this matter that would have avoided all of this rests upon both parties. If defense counsel had at any point (including going back to the issuance of the Rule 45 subpoena requiring that the computer be produced at the Minot Police Department) put forth a proposal for inspection that was compliant with what the federal rules permit, not based on inflated notions of relevancy and proportionality, and that set forth a protocol for inspection that preserved privacy interests, the result may have different. Likewise, if plaintiff's counsel had engaged in some additional dialog with defense counsel prior to taking the computer to the local computer store, it may have avoided that expense along with the present claims of spoilation, albeit as speculative as they might be at this point. In this case, both parties would have benefitted from spending less time letter writing and more time considering what the courts have concluded is reasonable as reflected by the cases cited later herein.

alternative, that the computer be turned over to defendants' expert for an intensive examination that would include recovery of any deleted files to the extent the files may still be recoverable. But, while defendants ask for relief in the alternative, it is clear that what they are really seeking is the forensic examination by their expert given the impracticality of plaintiff being able to respond to the requests as drafted.

II. DISCUSSION

Generally speaking, Fed. R. Civ. P. 34 treats discovery of electronic documents in the same manner as it treats discovery of paper documents. That is, the party seeking discovery of electronic information on a device belonging to the other party is normally not entitled to production of all of the electronic data on the device so that the party can rummage around looking for whatever the party might believe to be useful—even if the time frame is limited. Rather, the party seeking documentary evidence, whether it be in paper or in electronic format, must make specific requests for the documents it wants to obtain that "describe with reasonable particularity each items or category of items to be inspected" as required by Rule 34(b)(1)(A). Then, the party to whom the requests are made has the obligation to search for and produce the documents that are responsive and not subject to objection.

Not only is it clear from the text of Rule 34 that this is the normal course to be followed in the production of electronic information, the Official Advisory Committee Notes to the 2006 Amendments to Rule 34 Subdivision (a), in relevant part, state:

> Rule 34(a)(1) is also amended to make clear that parties may request an opportunity to test or sample materials sought under the rule in addition to inspecting and copying them. That

> opportunity may be important for both electronically stored information and hard-copy materials. The current rule is not clear that such testing or sampling is authorized; the amendment expressly permits it. As with any other form of discovery, issues of burden and intrusiveness raised by requests to test or sample can be addressed under Rules 26(b)(2) and 26(c). *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 documents and 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.*

(italics added).

As an initial matter, it not clear from defendants' predicate to its discovery requests whether defendants are asking for all the electronic information for each of the specified requests, *including* that related to the specific subject matters set forth in the predicate, or whether the requests seeking information beyond mere technical data are limited to the specified subject matters. If it is the former, the court agrees that defendants' requests are objectionable because, among other things, they seek all information, even if limited to a 60-day window, and not just that which would be relevant to the case. Consequently, the court will assume it is the latter.

While not entirely clear, it appears that plaintiff's attorneys voluntarily turned over any information that was recovered from the computer by its local expert within the 60-day window, even if it went beyond the subject matters specified in the predicate, while preserving in the formal written responses their objections to the scope and breadth of what was being requested as well objecting to any further examination. The question now is whether defendants are entitled to an exhaustive forensic examination of the computer since, as already noted, plaintiff making a detailed written response to the requests is not a realistic one.

The cases applying Rule 34 make clear that a party who is dissatisfied with Rule 34 discovery responses and seeks a forensic examination of a particular electronic device must (1) offer something more than suspicion that the device contains material that is relevant, and (2) that the forensic examination is proportional to the needs of the case in light of the factors set forth in Fed. R. Civ. P. 26(b)(1), including the additional costs and burdens imposed by such an examination. An often-cited case in this regard is the Sixth Circuit decision in John B. v. M.D. Goetz, Jr., 531 F.3d 448 (6th Cir.2008), where the court stated in relevant part:

> To be sure, forensic imaging is not uncommon in the course of civil discovery. See Balboa Threadworks, Inc. v. Stucky, No. 05–1157–JTM–DWB, 2006 WL 763668, at *3 (D.Kan. March 24, 2006). A party may choose on its own to preserve information through forensic imaging, and district courts have, for various reasons, compelled the forensic imaging and production of opposing parties' computers. See, e.g., Ameriwood Indus., Inc. v. Liberman, No. 4:06CV524–DJS, 2006 WL 3825291, at *3–*6 (E.D.Mo. Dec.27, 2006), amended by 2007 WL 685623 (E.D.Mo. Feb.23, 2007); Cenveo Corp. v. Slater, No. 06–CV–2632, 2007 WL 442387, at *1–*3 (E.D.Pa. Jan. 31, 2007); Frees, Inc. v. McMillian, No. 05–1979, 2007 WL 184889, at *2 (W.D.La. Jan.22, 2007). Nevertheless, "[c]ourts have been cautious in requiring the mirror imaging of computers where the request is extremely broad in nature and the connection between the computers and the claims in the lawsuit are unduly vague or unsubstantiated in nature." Balboa Threadworks, 2006 WL 763668, at *3; see also Balfour Beatty Rail, Inc. v. Vaccarello, No. 3:06–CV–551–J–20MCR, 2007 WL 169628, at *2–*3 (M.D.Fla. Jan.18, 2007); Diepenhorst v. City of Battle Creek, No. 1:05–CV–734, 2006 WL 1851243, at *2–*4 (W.D. Mich. June 30, 2006). As the Tenth Circuit has noted, albeit in an unpublished opinion, mere skepticism that an opposing party has not produced all relevant information is not sufficient to warrant drastic electronic discovery measures. See McCurdy Group, LLC v. Am. Biomedical Group, Inc., 9 Fed.Appx. 822, 831 (10th Cir.2001). And the Sedona Principles urge general caution with respect to forensic imaging in civil discovery:
>
> > Civil litigation should not be approached as if information systems were crime scenes that justify forensic investigation at every opportunity to identify and preserve every detail.... [M]aking forensic image backups of computers is only the first step of an expensive, complex, and difficult process of data analysis that can divert litigation into side issues and satellite disputes involving the interpretation of potentially ambiguous forensic evidence.
>
> The Sedona Principles, supra, at 34, 47. Thus, even 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. Cf. Fed.R.Civ.P. 34(a) Advisory Committee Note (2006) ("Courts should guard against undue intrusiveness resulting from inspecting or testing [electronic information] systems.").

Id. at 459–60. See also Tingle v. Herbert, Civ. No. 15-626, 2018 WL 1726667, at **6–8 (M.D. La. April 10, 2018) (denying a request for forensic examination of a cell phone and email accounts because it was based only on skepticism that discoverable information had not been produced, was lacking in proportionality, and failed to address the inherent privacy concerns); East Bridge Lofts Property Owners Association, Inc. v. Crum & Forster Specialty Insurance Company, No. 2:14-cv-2567, 2015 WL 12831731, at **2–3 (D.S.C. June 18, 2015) (concluding that a sufficient showing had not been made that warranted, at that point, a forensic examination); John Crane Group Corp. v. Energy Devices of Texas, Inc., No. 6:14-cv-178, 2015 WL 11089486, at *3 (E.D. Tex. February 2, 2015) (observing that "[d]irect inspection of an opponent's computers is generally the exception rather than rule" and denying a request for a forensic examination of the opposing party's computers because mere skepticism that discovery responses were not complete was not enough); NOLA Spice Designs, LLC v. Haydel Enterprises, No. 12-2515, 2013 WL 3974535, at **1–4 (E.D. La. Aug. 2, 2013) (denying request for forensic examination of computers because a sufficient threshold showing had not been made and the request lacked proportionality in relation to the needs of the case).

Aside from technical data with respect to the computer, including whether files and programs have been deleted, the content-based information that defendants appear to be seeking according to the predicate—at least as best the court can understand it—appears to fall within one of the

following five categories:

1. Information related to or evidencing methamphetamine possession, use, and/or trafficking of methamphetamine, including all references to the same by street names or slang, such as, but not limited to, “meth”, “crystal”, and “rock.”
2. Communications that Joshua Peterson had with other individuals in relation to methamphetamine.
3. Communications that Joshua Peterson had with other individuals in relation to buying and selling stolen goods.
4. Communications that Joshua Peterson had with:
   (a) Megan Owens;
   (b) Brandon Butler; and
   (c) the persons that Brandon Butler testified that he visited in the early morning hours on August 30, 2014.
5. Communications with anyone about the subject incident.

The predicate further states it is limited to information that is within a 60-day window of thirty days before the incident on August 30, 2014, and thirty days after.

With respect to the first two categories, the issue in this case is whether defendant Schmitt used excessive force in firing at the vehicle driven by plaintiff, severely injuring him. While plaintiff’s use of and dealing in drugs may be relevant to what he was doing at the time of the incident and may also be relevant generally in terms of the scope of potential damages, his use and

dealing of drugs is only relevant up to a point. And, in reviewing plaintiff's deposition, he has admitted to: (1) consuming methamphetamine on an almost daily basis for a number of years prior to the incident; (2) consuming methamphetamine throughout the day leading up to the incident; (3) renewing his consumption of methamphetamine after treatment following the incident and continuing to use it up to when he went to prison; and (4) dealing drugs (specifically methamphetamine) on the day of the incident as well as before and after, including the fact this was his only gainful employment. In short, defendants already have more information on the subject of plaintiff's drug use and drug dealing than the trial judge will likely allow to be admitted, particularly after balancing Rule 403 concerns.[2]

Likewise, the same is true for the third category, which is communications plaintiff may have had with others relating to the buying and selling of stolen goods. Plaintiff already admitted in his deposition that he was in the process of burglarizing Minot Welding just prior to the shooting. Except for any conversations plaintiff may have had with Butler about burglarizing Minot Welding

[2] Defendants may contend that some of the requested information related to drugs and drug dealing may be relevant in terms of being able to attack Butler's account of the events. However, Butler admitted during his deposition to being a regular user of methamphetamine and that he had been using it along with plaintiff over a number of hours leading up to the incident, as well as personally consuming upwards of ten cans of beer. And, while he attempted to deny in his deposition that he had ever been involved in dealing drugs, he acknowledged he pled guilty to possession of methamphetamine on the day of the incident with the intent to deliver. He also admitted that he was the one who purchased a certain quantity of methamphetamine on the day of the incident that in part he gave to plaintiff—which is drug dealing. Further, the physical evidence retrieved following the incident included bags of drugs marked with the prices that were recovered from Butler's backpack. Finally, plaintiff has himself testified to the drug transaction that he and Butler engaged in on the day of the incident and plaintiff's ex-wife also testified she had been supplied drugs by Butler. In short, this is not a drug conspiracy case; further details of the drug activity prior to the incident in terms of additional sales and the persons involved are collateral to the issues of this case. And, to the extent Butler's credibility is an issue, there is already more evidence than what the court is likely to allow on that score. Further discovery on these points is neither relevant nor proportional to the needs of the case.

prior to the incident, information about plaintiff buying and selling stolen goods is beside the point with respect to this case.

With respect to the fourth category, defendants appear to seek all information pertaining to conversations that plaintiff may have had with the persons specified. The requests here are overbroad in that they encompass communications that have nothing to do with the case and any relevant ones would be encompassed in the fifth category of information discussed next.

What may be of some relevance and not necessarily cumulative is what defendants seek in the fifth category. This includes any communications plaintiff had with others about the shooting incident and the events immediately associated with it, including the burglarizing of Minot Welding and the attempted flight by plaintiff and Butler.

But, as already noted, relevancy alone is not enough. Defendants must demonstrate there is a reasonable possibility amounting to more than surmise and conjecture that relevant and responsive information may still exist on the computer, which plaintiff's counsel were not able to retrieve, and that a forensic examination is proportional to the needs of the case. With respect to the fifth category, the court concludes there is enough to permit defendants to proceed with a forensic examination, including the following:

- The evidence that plaintiff used his computer for communicating with others before and after the incident. And, while it appears that most of the communications were likely from web-based platforms, there is the possibility that, for certain programs, copies of the communications may have resided on the computer and may still be

recovered even though nominally deleted.

- The evidence that one of the communication programs that plaintiff had used was not on the computer when it was examined by the local computer store and which the computer store stated could have been deleted.
- The evidence that plaintiff discussed the events surrounding the incident after-the-fact in person with Butler and likely others. Given that plaintiff was known to have communicated by computer, it is not a reach to conclude there may also have been similar communications using that medium.
- Plaintiff has admitted to engaging in criminal conduct both on the day of the incident as well as before and after. He also has admitted to carrying on several affairs with other women. Given this, it is also not a stretch to conclude that he may have been in the habit of deleting material from his computer (although, perhaps, not in a sophisticated enough fashion to completely wipe it to the point where it becomes irretrievable) and that this could have extended to the information that the court will permit to be searched for.
- Plaintiff's ex-spouse admitted that she deleted some information from the computer while it was in her possession following the incident and the extent to which she may have done so is not certain.
- Plaintiff contends he has no memory of what happened after he saw the police car pull up outside of Minot Welding and his thinking to himself he needed to get out of

> there. Plaintiff contends this lack of memory is due to the traumatic nature of the shooting. However, while plaintiff's account has a ring of authenticity—particularly in view of everything else he has said and the fact that this puts him in the position of personally not being able to dispute the accounts of the officers involved, plaintiff has a demonstrated history of untruthfulness. The court cannot discount the possibility of his having offered more detail about the incident in subsequent communications with others.

In summary, while there is no reason to suggest that plaintiff's counsel have withheld any responsive information that they were able to retrieve with the help of their expert, defendants have offered enough to demonstrate a reasonable possibility amounting to more than mere conjecture that material that is now discoverable may have been on the computer and deleted prior to the computer coming into the possession of plaintiff's counsel.

The examination that the court will permit will be limited to a search for: (1) any communications that plaintiff had with anyone about burglarizing Minot Welding during the period from May 28 through May 30, 2014, and (2) any communications or documents that mention or relate to the burglary of Minot Welding, the attempted flight by plaintiff and Butler, and the shooting. With respect to the latter, the court will not impose a time limitation, since any communications by plaintiff about the incident, even after the 30 days following the incident, may be of some relevance.

While the court will order that plaintiff's attorneys make the computer available to

defendant's expert for further examination, it will not allow defendants' attorneys free access to any information that might be on the computer through the expert they have retained. Consequently, to address the privacy concerns noted in the cases previously cited, the examination will be limited in terms of content, and the protocol for the search and production of any responsive information shall be as set forth in the court's order below, which is on par with what this court and others have ordered. See, e.g., Bellisle v. Landmark Medical Center, No. 14-266, 2015 WL 13672466, at *2 (D.R.I. Nov. 16, 2015) (ordering a similar protocol); Weatherford U.S., LP v. Innis, No. 4:09-cv-061, 2011 WL 2174045, at * 5 (D.N.D. June 2, 2011) (adopting a similar protocol and citing Ameriwood Indus., Inc. v. Liberman, No. 4:06CV524–DJS, 2006 WL 3825291, at **5-6 (E.D. Mo. Dec. 27, 2006); Antioch Co. v. Scrapbook Border, Inc., 210 F.R.D. 645, 653–54 (D. Minn. 2002), Simon Property Group L.P. v. mySimon, Inc., 194 F.R.D. 639, 643–44 (S. D. Ind. 2000), and Playboy Enterprises. v. Welles, 60 F. Supp. 2d 1050, 1054–55 (S.D. Cal.1999)).

III. ORDER

Based on the foregoing, defendants Motion to Compel (Doc. No. 67) is **GRANTED IN PART** and **DENIED IN PART**, and the court **ORDERS** as follows:

1. The court will permit a forensic examination of plaintiff's laptop computer but limited to the following:

   a. A search for (1) any communications that plaintiff had with anyone about any attempts to commit theft or burglary of Minot Welding during the period from May 28 through May 30, 2014, and (2) any communications or documents that mention

or relate to the burglary of Minot Welding, the attempted flight by plaintiff and Butler from the scene, and the shooting.

b. Electronic information relevant to when and how the foregoing information was stored or deleted and how it was recovered.

2. Plaintiff's counsel shall ship at defendants' expense the laptop computer to defendants' forensic expert. The risk of loss or physical damage to the computer shall at all times be upon the defendants from the time it is turned over by plaintiff's counsel to the shipping company until it is returned to plaintiff's counsel.

3. The protocol for the search, retrieval, and production of any responsive information shall be as follows:

a. Defendants' expert may image the computer for purposes of the examination and may retain custody of the image, subject to the requirements of non-disclosure set forth below, until a final non-appealable judgment has been entered in this case, at which point the image must be destroyed.

b. Except as provided below, defendants' expert may not share any of the information obtained from the examination with any person, including defendants' counsel.

c. Any documents or other responsive information that defendants' expert retrieves from the computer the contents of which appear to fall within the subject matters of the search being permitted as set forth above shall be sent by the expert to *plaintiff's counsel* in a format that will enable them to review it. Plaintiff's counsel will then

have twenty days to review and produce the information that falls withing the scope of the subject matters delineated above. If plaintiff's counsel believes the material should not be produced because it either is not within what the court has ordered or there is some other basis for objection, plaintiff's counsel shall submit the withheld material to the court for an *in camera* inspection and file a brief setting forth the bases for not producing the information.

d. Defendants' expert may disclose to defendants' attorneys whether any information was turned over to plaintiff's counsel (without disclosing the contents of the information), where it came from, whether any of it came from data that was deleted, and when the deletions took place. Also, defendants' expert can communicate whether any programs appear to have been deleted and, if so, when. If based on this information as well as whatever might ultimately be produced by plaintiff's counsel, defendants' counsel believes there are good reasons why they should be entitled to more information, they can request a hearing on the matter.

e. Prior to any shipment of the computer for examination, defendants' attorneys must file with the court a declaration by defendants' expert in which he agrees not to communicate the contents of any information that he has reviewed or retained to any person(s), including defendants' counsel, without a prior order of the court. The only exceptions are the transmittal of any responsive information to plaintiff's counsel as well as the communication of certain non-content information to defendants' counsel

as set forth above. The declaration must be sworn to under oath and shall contain a statement that defendants' expert submits himself to the jurisdiction of this court for purposes of compliance with this court's orders, including the court's exercise of its contempt power in the event of any noncompliance by the expert with this order or any other order the court may issue involving the computer and the information extracted from it.

f. Defendants shall bear the cost of the forensic examination. Upon completion of the examination, defendants' expert shall promptly ship the computer back to plaintiff's counsel at defendants' expense.

Dated this 21st day of September, 2018.

/s/ Charles S. Miller, Jr.
Charles S. Miller, Jr., Magistrate Judge
United States District Court