

United States v. Gardner

Decided Dec 21, 2012

Case No. 2:10-CR-551-TC

12-21-2012

UNITED STATES OF AMERICA, Plaintiff, v. BRYAN JAMES GARDNER, Defendant.

TENA CAMPBELL

ORDER

AND

MEMORANDUM DECISION

Defendant Bryan James Gardner has been charged with one count of possession of child pornography and one count of distribution of child pornography. Mr. Gardner notified the United States that he intends to rely on the testimony of Steven Moshlak, whom Mr. Gardner has designated as an expert in computer forensics. Although the United States does not challenge Mr. Moshlak's qualifications as a computer forensics expert, it does challenge, under [Federal Rule of Evidence 702](#) and [Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579](#) (1993), Mr. Moshlak's application of the methodology used and the reliability and relevancy of the opinions he offers in his report.

The court held a [Daubert](#) hearing at which Mr. Moshlak testified. Based on Mr. Moshlak's testimony, the content of his report (as amended), and the parties' arguments, the court holds that Mr. Moshlak will be allowed to testify as an expert witness at trial but his testimony will be limited to a narrower set of conclusions than was proffered in his report. As set forth below in more detail below, the United States's Motion to Exclude

2 Testimony of *2 Defendant's Expert Steven Moshlak¹ is GRANTED IN PART AND DENIED IN PART.

¹ Docket No. 210.

BACKGROUND

Defendant Bryan Gardner is charged with possessing child pornography images on the Gardner family computer (Count 1) and distributing child pornography images by uploading images to the social networking Internet site Ning.com using a Verizon wireless (wi-fi) Internet access device (Count 2).

Mr. Moshlak is knowledgeable about computer forensics, as demonstrated by his Curriculum Vitae and information gleaned during the court's [Daubert](#) hearing. (See Curriculum Vitae of Steven Moshlak (Def. Ex. A); Dec. 3, 2012 [Daubert](#) Evidentiary Hr'g Tr. (Docket No. 262) ("Tr.") at 200-201.) The United States does not

challenge his credentials as a computer forensics examiner.

Mr. Moshlak, as Mr. Gardner's designated expert witness, reviewed the same forensic images of two hard drives that were seized and reviewed by the United States's investigators and computer forensics experts. The hard drives were taken from the Gardner family computer (one was seized from the Gardner home and the other was seized at PC Laptops, where the drive was being repaired at the time the search warrant was executed). The computer investigation concerning Count 1 centers on the contents of the hidden thumbs.db file, as well as the email address kidpower12345@yahoo.com. The investigation concerning Count 2 focuses on the social networking site Ning.com, two email addresses (kidpower12345@yahoo.com and
3 kidpower2009@live.com), the website imgsrc.ru (referred to as "Image Source"), and a wi-fi *3 device.

Mr. Moshlak primarily used the AccessData software called Forensic Toolkit (FTK) to do his review. That is the same program used by the Government's computer forensics experts at the FBI's Intermountain West Regional Computer Forensics Laboratory (IWR CFL or RCFL). Understandably, the Government does not challenge the soundness of the FTK methodology.

Mr. Moshlak also reviewed discovery materials provided by the Government to Mr. Gardner, and he apparently did his own research and investigation above and beyond his forensic examination of the hard drive images (for example, by contacting Verizon about the type of modem allegedly used by Mr. Gardner). (See Tr. 252 (testifying that he received the modem information from Verizon, saying, "I came across a code, talked to [Verizon] about it, and they [Verizon] told me that during the time frame that Mr. Gardner would have purchased the USB [modem], this is the unit they were offering.").

The end result of his investigation and analysis is memorialized in his "Computer Expert Witness Report" (dated September 30, 2012) and his November 22, 2012 "Addition, Changes and Modifications to the Defendant's Computer Forensics Expert Witness Report." (See Def. Exs. B & B-1.) Mr. Moshlak, in his report, sets forth roughly fourteen conclusions.² During the Daubert hearing, he elaborated on the content of his report and his conclusions, all of which are challenged by the United States. The Government contends that Mr. Moshlak's testimony is neither relevant nor reliable because "he relied on insufficient data, incorrectly applied
4 *4 methodologies, made unsupported assumptions, and many of his conclusions are simply irrelevant to the facts at issue in this case." (U.S. Mem. Supp. Mot. Exclude Moshlak Testimony (Docket No. 251) at 2.)

² Mr. Moshlak's original report listed thirteen conclusions (some of which had multiple parts), but the recent amendment to his report added an independent conclusion to the original report's item number 6. (See Def. Ex. B at 84; Def. Ex. B-1 at A-4.) The court refers to those conclusions as 6(A) and 6(B).

ANALYSIS

Rule 702 of the Federal Rules of Evidence, which governs the admissibility of testimony by expert witnesses, provides that:

A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:

- (a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
- (b) the testimony is based on sufficient facts or data;
- (c) the testimony is the product of reliable principles and methods; and
- (d) the expert has reliably applied the principles and methods to the facts of the case.

Fed. R. Evid. 702. Under Rule 702, the court typically performs a two-step analysis to determine whether the challenged expert opinion is admissible: first, the court must determine whether the expert is qualified to state an opinion in the area for which he has been designated an expert; second the court must determine whether the proffered opinion is reliable under Rule 702 and the principles set forth in Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993). 103 Investors I, L.P. v. Square D Co., 470 F.3d 985, 990 (10th Cir. 2006). Because Mr. Moshlak's testimony has been challenged, Mr. Gardner, as the proponent of the testimony, bears the burden of establishing that the proffered testimony is admissible under the Daubert guidelines. United States v. Nacchio, 555 F.3d 1234, 1241 (10th Cir. 2009). *5

Here, the United States does not challenge Mr. Moshlak's credentials as a computer forensics expert or the methodology he used (i.e., computer forensic examination using Forensic Tool Kit). But the United States contends that Mr. Moshlak's conclusions are neither reliable nor relevant and so he should not be allowed to testify at all during trial.

"Under Rule 702, a district court must satisfy itself that the proposed expert testimony is both reliable and relevant, in that it will assist the trier of fact, before permitting a jury to assess such testimony." United States v. Rodriguez-Felix, 450 F.3d 1117, 1122 (10th Cir. 2006). In determining reliability, the court may look at the expert's data, method, or application of the method to the data. "Under Daubert, 'any step that renders the [expert's] analysis unreliable . . . renders the expert's testimony inadmissible. This is true whether the step completely changes a reliable methodology or merely misapplies that methodology.'" Mitchell v. Gencorp Inc., 165 F.3d 778, 782 (10th Cir. 1999) (quoting In re Paoli R.R. Yard PCB Litigation, 35 F.3d 717, 745 (3d Cir. 1994)). The court will address each of Mr. Moshlak's conclusions in the order presented in his report. **Expert Conclusion 1. Multiple users, including members of the Gardner family and parties outside the Gardner household, accessed and used the Gardner family computer.**

Here, Mr. Moshlak presumes there were multiple users of the computer (family members and possibly others outside the Gardner household) based on the existence of computer directories and files bearing different names and containing resumés of individuals other than Mr. Gardner. Even though the United States agrees that several members of the Gardner family had access to the computer (based on statements by family members), the court will not allow Mr. Moshlak to testify about his conclusion as it is presently worded. As written, his conclusion *6 is not an expert conclusion based on scientific, technical, or other specialized knowledge. Whether more than one person, and, if so, who, used the computer, is a fact question for the jury to decide. Mr. Moshlak's proffered testimony would usurp the role of the jury. Mr. Moshlak, however, will be allowed to testify that during his review of the Gardner family computer, he observed files, directories, and documents with names other than Bryan Gardner. He may not extrapolate further. **Expert Conclusion 2. "HP Owner" was the generic user name assigned to anyone accessing the family computer.**

This conclusion is relevant. But the court is concerned with the phrasing used by Mr. Moshlak. The court will allow Mr. Moshlak to state his opinion, but only if it is framed in a way that more accurately reflects the nature of the fact (and to the extent it is not cumulative). That is, rather than stating that the "HP_Owner" was not associated with Mr. Gardner, Mr. Moshlak may point out that the "HP_Owner" name was not associated with or assigned to any particular individual using the computer. **Expert Conclusion 3. No Relative Identifiers (RIDs) or Security Identification Descriptors (SIDs) were associated with Mr. Gardner on the family computer.**

The analysis of Conclusion 2 also applies here. The court finds the lack of RIDs and SIDs to be somewhat relevant. However, Mr. Moshlak may not present his opinion in the matter phrased in his report. He may point out to the jury that there are no RIDs or SIDs associated with anyone on the Gardner family computer. This is more accurate than the artificial spin he places on the lack of RIDs and SIDs in an effort to eliminate Mr.

7 Gardner as a possible user of the family computer. *7 **Expert Conclusion 4. A peer-to-peer network was found on the family computer, but it was apparently used primarily for downloading music-related material.**

The United States does not contend that any child pornography image was downloaded or uploaded through a peer-to-peer network. For this reason, Mr. Gardner admits that the existence of a peer-to-peer music sharing program on the computer is "not directly relevant[.]" (Def.'s Response to US's Mot. Exclude Expert Testimony (Docket No. 260) at 4.) But Mr. Gardner asserts that "this information when combined with testimony that brother Daniel Gardner had over 20,000 music files on the family machine at one time is relevant to who used the computer and with what frequency." (Id.) The court disagrees.

Mr. Moshlak's conclusion as presented in his report—i.e., that a peer-to-peer network was being used essentially only for downloading music—would be distracting and confusing to the jury. The immediate inference one takes away from Mr. Moshlak's emphasis is that the peer-to-peer network was not used for downloading pornographic images. But that proves nothing of consequence in this case because the United States does not allege that Mr. Gardner used a peer-to-peer network to download or store offending images. The way the conclusion is worded would not be helpful to the jury. Also, Mr. Moshlak's finding adds nothing to the defense's theory that another person's frequent use of the computer lessens the likelihood that Mr. Gardner was the one who possessed or distributed child pornography. Defense admits that there is separate evidence of Daniel Gardner's 20,000 music files on the family computer.

8 Mr. Moshlak's observation is cumulative at best, and would not be helpful to the jury. Accordingly, he may not testify about this fourth conclusion. *8 **Expert Conclusion 5. The RCFL report did not identify any actors and so the report, as well as the analysis of Government agents who generated the report, is insufficient.**

The court agrees with the United States that this conclusion is not relevant, not based on scientific, technical or other specialized knowledge, and is not based on sufficient facts or data. The RCFL computer forensics examiners do not do investigative work. Mr. Moshlak's conclusion assumes that they are required to do so in order to do their jobs effectively. But the type of investigation to which Mr. Moshlak is referring was not part of the RCFL experts' scope of work. Moreover, Mr. Moshlak has no specialized expertise regarding the job of a government computer forensic examiner. As the United States notes, the Department of Justice guide for law enforcement is not sufficient data for Mr. Moshlak to speculate about what individuals involved with this case should have done. The court excludes any testimony of this nature. **Expert Conclusion 6(A). RCFL examiners erred in their failure to provide a detailed analysis in their report.**

For the same reasons set forth under Conclusion 5, the court excludes Mr. Moshlak's testimony on his Conclusion 6(A). **Expert Conclusion 6(B). The image modification dates in the thumbs.db file suggest that Mr. Gardner could not have downloaded or viewed the images because the dates coincide with the dates Mr. Gardner was in prison.**

Based on a long colloquy during the Daubert hearing, Mr. Moshlak admitted that the modification dates in the thumbs.db file do not have any bearing on whether Mr. Gardner downloaded or viewed the images on the Gardner family computer. (See Tr. 176 ("thumbs.db is unreliable insofar as looking at it from a date

9 perspective").) Accordingly, this conclusion is excluded as unhelpful to the jury. *9 **Expert Conclusion 7. The thumbs.db is a hidden file in the Gardner family computer that cannot be accessed without specialized computer knowledge and tools.**

This conclusion is not relevant. The Government does not contend that Mr. Gardner accessed the thumbs.db file to store or view child pornography images. The conclusion, while accurate, would not be helpful to the jury. In fact, it would be confusing. It suggests that Mr. Gardner could not have done what the Indictment alleges because he does not have specialized knowledge or tools to access the thumbs.db file. This testimony is excluded. **Expert Conclusion 8. The RCFL examiners erred in failing to provide a narrative analysis in their report.**

For the same reasons set forth under Conclusion 5, the court excludes Mr. Moshlak's testimony on his Conclusion 8. **Expert Conclusion 9. The Yahoo Companion toolbar has a button for kidpower12345@yahoo.com that allows anyone to access the email account.**

The United States contends that although "[t]he fact that kidpower12345 is in Yahoo Companion is not disputed, the conclusion about how it works is not based on sufficient facts or reliable methodologies." (U.S.'s Mem. Supp. Mot. Exclude Expert Testimony (Docket No. 251) at 9.) The court agrees.

As part of his conclusion, Mr. Moshlak testified that "anybody that goes ahead and activates a Web browser has the ability to go ahead and log in as kidpower12345[.]" (Tr. 193.) Mr. Moshlak provided no factual basis for such a conclusion or any reason for the court to believe that he has expertise regarding the Yahoo Companion toolbar or that he can explain why he reached this conclusion. Because Mr. Moshlak's Conclusion 9 was
10 unsupported, it is *10 excluded at this time. The court will reconsider this ruling if the defense is able to provide the court with a more thorough analysis and a complete record in support. **Expert Conclusion 10(A). The wi-fi device allegedly used by Mr. Gardner was a Verizon Wireless USB727 modem with a VZAccess Manager enhancement.**

Mr. Gardner speculates in this conclusion based on "what-ifs" and a conversation he had with an unidentified person at Verizon. He is not allowed to parrot hearsay. This conclusion is excluded. **Expert Conclusion 10(B). Conclusions based on IP Addresses**

In his report, Mr. Moshlak states,

No traceroute data analysis was provided, as to the network which was used, in determining if a nexus between the Defendant and his USB modem could be established. In review of the material provided [sic] shows no Verizon Access Manager connectivity, but does show QWEST as a potential provider of services. In addition an IP address analysis was performed based upon the Username logons and user names provided [by] Ning, and the IP address data that was provided in this case, with the user logon, related to a number of different areas in the nation. A number of these IP addresses resolved to various other parts of the nation, including [over twenty locations within the United States].

(Moshlak Report (Def.'s Ex. A) at 87.) Defendant has failed to show that Mr. Moshlak's IP address analysis was based on sufficient facts or data. The source of information and the nature of the conclusion are both in question. The IP address analysis and conclusions do not make sense. On the stand, Mr. Moshlak himself admitted that he did not know how someone could log-in over 300 times on a particular date or from multiple locations throughout the country. He said, "something tells me something isn't right. We ought to go back and take a look at it." (Tr. 198.) Unless and until the defense can come up with a more thorough analysis and

11 explanation for the conclusion, Mr. Moshlak's testimony in this area is excluded. *11 **Expert Conclusion 11. The cybertips from Ning.com need more investigation.**

For the same reasons set forth under Conclusion 5, the court excludes Mr. Moshlak's testimony on his Conclusion 11. **Expert Conclusion 12. The Government's investigation did not describe the details of the work performed by PC Laptops on the Gardner family computer.**

To the extent Mr. Moshlak is criticizing the Government's investigation techniques, his testimony is not admissible, essentially for the same reasons set forth under Conclusion 5. The fact that the hard drive was seized from PC Laptops may have a sliver of relevance to Mr. Gardner's theory that someone else was responsible for the images on the computer, but the conclusion offered is not based on any scientific, technical or specialized knowledge and so Mr. Moshlak may not testify about this subject. **Expert Conclusion 13. There were viruses on the Gardner family computer.**

During testimony, Mr. Moshlak admitted under cross-examination that the viruses could not have created the images of child pornography in the thumbs.db folder. (Tr. 263.) Absent any evidence (other than the speculation offered by the Defendant) that a third party hacked into the Gardner family computer to download the offending images, Mr. Moshlak's conclusion is, at best, not relevant, and would confuse the jury.

CONCLUSION

The court will not fully exclude Mr. Moshlak's testimony at this time. However, to the extent he attempts to testify beyond his credentials as a computer forensics expert (e.g., by making conclusions based on his own investigation and analysis of non-computer-related data), the court will not allow it. He has been designated
12 and approved as an expert in a narrow area of *12 expertise.³ Anything else is either not supported by scientific, technical, or specialized knowledge, or is simply not relevant. The court notes that some parts of Mr. Moshlak's conclusions are not disputed by the United States. To the extent the defense presents Mr. Moshlak's testimony about evidence already in the record, the court will not allow his testimony on the basis that it is cumulative.

³ During the Daubert hearing, Mr. Moshlak defined computer forensics as "a specialized practice in investigating computer media for the purpose of discovery, analyzing available hidden or deleted data information that may serve as useful evidence in a legal matter." (Tr. 170-71.)

ORDER

For the foregoing reasons, the United States's Motion to Exclude the Expert Testimony of Steven Moshlak (Docket No. 210) is GRANTED IN PART AND DENIED IN PART.

BY THE COURT:

TENA CAMPBELL

U.S. District Court Judge
