

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

JOHN W. FERRON,

Plaintiff,

v.

Case No. 2:06-cv-327

JUDGE GREGORY L. FROST

Magistrate Judge Mark R. Abel

SEARCH CACTUS, L.L.C., et al.,

Defendants.

OPINION AND ORDER

The Court held a telephone conference in this action on April 14, 2008, in which all parties were represented and this Court considered and decided the protocol for viewing and preserving information contained on Plaintiff's computer systems. This Opinion and Order memorializes that decision.

I. Background

Plaintiff is an attorney who utilizes his home and office computers for storing and working with information related to the representation of clients, the maintenance of lawsuits such as this action and other actions or potential actions similar to the subject matter of the instant action, and his personal life. Out of these three categories of information, the information related to the representation of clients in cases unrelated to email and advertising litigation has no relevance to this case and contain documents that are protected by the attorney-client privilege. The information that may be categorized as personal also has no relevance to this case and may be confidential in nature, *e.g.*, banking and credit card information. However, the third category of information, *i.e.*, information related to email and website advertising litigation is

relevant and discoverable.¹ *See* Fed. R. Civ. P. 26(b) (information is admissible or is reasonably calculated to lead to the discovery of admissible evidence).²

In this Court's Opinion and Order which granted in part and denied in part Defendant Search Cactus' motion for summary judgment, it held that "only the *unsolicited* emails Plaintiff received at jferron@ferronlaw.com after April 3, 2006 can be used to support his claim under the [Ohio Consumer Sales Practices Act] OCSPA." (Doc. # 237 at 17) (emphasis in original). Thus, it is necessary for the parties to ascertain which of the emails Plaintiff received were unsolicited. As Defendants contend, Plaintiff's computer systems contain the only available documentary evidence that can show the pathways taken by Plaintiff to solicit the emails or the absence of those pathways.

II. Defendants' Discovery Requests

Defendants have requested an inspection of Plaintiff's computer systems so as to capture specific information relevant to this case that Plaintiff has not produced and, Defendants contend has not been placed on a litigation hold. Specifically, Defendant wishes to inspect Plaintiff's

¹ The Court notes that, on March 11, 2008, Plaintiff timely objected to Media Breakaway, LLC's "Second Set of Requests for Production and to Permit Inspection of Documents and Other Tangible Things," which sought inspection of the computers Plaintiff uses. Plaintiff noted the following objections to Media Breakaway, LLC's request to inspect the computers: "This Request is overly broad and unduly burdensome. This Request to Inspect does not seek information that is relevant to either the claims or defenses in this matter, or likely to lead to the discovery of relevant evidence. This Request seeks information protected by the attorney-client and/or work product privileges." Plaintiff continues to object to Media Breakaway, LLC's inspection of the computers upon these bases.

² The Court notes that Plaintiff continues to object to Media Breakaway, LLC's request for discovery of this category of information upon the asserted basis that Plaintiff's solicitation of commercial advertisements is not relevant for purposes of determining whether Plaintiff states claims under the Ohio Consumer Sales Practices Act.

computer systems to ascertain whether Plaintiff's efforts with respect to receiving the emails and visiting the websites (that are at the heart of this action) constituted a consumer transaction under the OCSPA, or whether Plaintiff's opening of the emails and any attempts to obtain free merchandise were part of a business designed to profit from email litigation

The parties agree that a forensic computer expert must be utilized to obtain the information that the Court has determined Defendants are entitled to discover.³ This is because a distinctive feature of computer operations is the routine alteration and deletion of information that attends ordinary use of the computer. Many steps essential to computer operation may alter or destroy information, for reasons that have nothing to do with how that information might relate to litigation. As a result, the ordinary operation of computer systems creates a risk that a party may lose potentially discoverable information without culpable conduct on its part. The routine operation of computer systems includes the alteration and overwriting of information, often without the operator's specific direction or awareness, a feature with no direct counterpart in hard-copy documents. Such features are essential to the operation of electronic information systems. *See Fed. R. Civ. P. 37 Advisory Committee's Note on 2006 Amendments* (explaining some of the differences in computer discovery as opposed to paper discovery). On March 19, 2008, this Court held a telephone conference with the parties, directed that inspection of

³ The Court also notes that the parties disagree about the types of information that must be analyzed on the computers in order to reconstruct internet browser history. Plaintiff's computer consultant has attested that the internet browsing history may be re-constructed through a limited examination of certain directories on the computers' hard drive. Defendant's computer consultant has attested that such an analysis can only occur by analyzing a complete mirror image of the hard drives of the computers.

Plaintiff's computer systems' hard drives⁴ was appropriate, and instructed the parties to discuss and propose a protocol for the inspection.

III. Analysis

The parties were unable to agree on a protocol for inspection of Plaintiff's computer systems' hard drives and requested another conference with this Court to address the issue. At the April 14, 2008 telephone conference, this Court considered the parties' arguments related to the inspection of Plaintiff's computers. The issues of concern were how to protect Plaintiff's confidential personal information that is stored on the computers, *e.g.*, personal banking and credit card information, and how to prevent Plaintiff from waiving the attorney-client privilege by allowing the information on the computers to be viewed by any third party.

Initially, the Court explains that the 2006 amendments to Rule 34 of the Federal Rules of Civil Procedure clarify "that discovery of electronically stored information stands on equal footing with discovery of paper documents." Fed. R. Civ. P. 34 Advisory Committee's Note on 2006 Amendments. Consequently, without a qualifying reason, Defendants are no more entitled to access to Plaintiff's electronic information storage systems than to Plaintiff's warehouses storing paper documents. *See Scotts Co., LLC v. Liberty Mut. Ins. Co.*, No. 3:06-cv-899, 2007 U.S. Dist. LEXIS 43005, at *4-5 (S.D. Ohio June 12, 2007) ("the 2006 amendments to Rule 34 do not require the requested discovery order as a matter of course"); *Diepenhorst v. City of Battle Creek*, No. 1:05-cv-734, 2006 U.S. Dist. LEXIS 48551, at *10-11 (W.D. Mich. June 30, 2006) (same). *See also* 7-37A Moore's Federal Practice - Civil § 37A.44 (explaining electronic

⁴ If Defendants' review of Plaintiff's hard drives reveals that Plaintiff has removed discoverable information from the hard drives, the parties shall decide the process for review of Plaintiff's back-up tapes, drives, or servers from which the information can be retrieved.

discovery).

Here, the Court concludes that there are qualifying reasons sufficient to permit Defendants access to Plaintiff's computer systems: Plaintiff has apparently failed to fulfill his "duty to preserve information because of pending or reasonably anticipated litigation," Fed. R. Civ. P. 37 Advisory Committee's Note on 2006 Amendments, and Plaintiff has not otherwise produced the relevant information. Moreover, the fact that Plaintiff's computers contain the only available documentary evidence of his visits to the websites in issue and such evidence has not otherwise been produced, distinguishes this case from *Scotts* and *Diepenhorst*. In *Scotts*, the court stated that "plaintiff seeks to compel the re-production of electronically stored information previously produced by defendant in hard copy form." 2007 U.S. Dist. LEXIS 43005, *3. Likewise, in *Diepenhorst*, the court found that plaintiff had already produced the requested material, presumably also in hard copy form. 2006 U.S. Dist. LEXIS 48551, at *11.

Plaintiff takes the position that he did in fact place a proper litigation hold on electronically stored information relating to this case. Specifically, Plaintiff has represented to the Court that he has saved and preserved all of his commercial email since January 1, 2006. Plaintiff also represents to the Court that no Defendant in this case has ever requested that he place a litigation hold on any other type of electronically stored information resident on his computers. Lastly, Plaintiff represents to the Court that Plaintiff has never received any notice that Defendant intended to inspect the computers he uses to retrieve this information until he received Media Breakaway, LLC's formal discovery requests on February 7, 2008. Plaintiff's arguments are not well taken.

Even if Plaintiff has preserved and saved his “commercial email,” those actions do not sufficiently fulfill his duty to preserve evidence, which “arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation.” *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003) (quoting *Fujitsu Ltd. v. Federal Express Corp.*, 247 F.3d 423, 436 (2d Cir. 2001)). Further, Plaintiff’s duty to preserve this information is independent of whether Defendants requested a litigation hold. *See id.*; *see also Kemper Mortgage Inc. v. Russell*, No. 3:06-cv-042, 2006 U.S. Dist. LEXIS 20729, at *3 (S.D. Ohio Apr. 18, 2006) (“While that obligation may be enforced by court order or by a later sanction for spoliation, obviously the duty arises independent of any court declaration of the duty and indeed long before a court is available to make a declaration in the particular case.”).

The Court will now consider Plaintiff’s concerns regarding this Court’s order allowing inspection of Plaintiff’s computer systems’ hard drives.

A. Confidential Personal Information

The parties and this Court agree that Plaintiff’s personal information is confidential in nature and is irrelevant to this lawsuit. Defendants request a current mirror image⁵ of Plaintiff’s computer systems’ hard drives, contending that Plaintiff’s removal of any information from the computer hard drives can unwittingly cause deletion of other, possibly relevant, information.

This Court attempts to strike a balance between protecting Plaintiff’s personal confidential information and Defendant’s allegation that deletion can cause a loss of data.

⁵A mirror image copy represents a snapshot of the computer’s records. 7-37A Moore’s Federal Practice - Civil § 37A.03[1]-[3]. It contains all the information in the computer, including embedded, residual, and deleted data. *See id.*

Indeed, in a case in the Western Division of this District, the court declined to take a position on whether mirror imaging of hard drives was necessary to satisfy the preservation duty. *See Kemper Mortgage Inc. v. Russell*, No. 3:06-cv-042, 2006 U.S. Dist. LEXIS 20729, at *4-6 (S.D. Ohio Apr. 18, 2006). To strike a balance between these competing interests, this Court **ORDERS** Plaintiff's forensic computer expert⁶ to mirror image both of Plaintiff's computer systems' hard drives and for Plaintiff to store the images safely. Plaintiff's forensic computer expert shall then remove only Plaintiff's personal confidential information that could not reasonably lead to the discovery of information relevant to this litigation. Plaintiff shall provide Defendants with the protocol his expert utilized to remove the confidential information.

B. Attorney-Client Privileged Information

Plaintiff argues that if he is required to allow Defendants' forensic computer expert⁷ to review and copy Plaintiff's computer systems' hard drives, it will simultaneously cause the loss of the attorney-client privilege that has attached to the information related to Plaintiff's other clients because that information will be viewed by a third party. This Court disagrees.

First, the Court notes that it is Plaintiff himself that has caused this issue to become problematic because of his failure to place a sufficient litigation hold on his computer systems as of the date he anticipated this litigation. *See Fed. R. Civ. P. 37 Advisory Committee's Note on 2006 Amendments; Thielen v. Buongiorno USA, Inc.*, No. 1:06-cv-16, 2007 U.S. Dist. LEXIS 8998, at *8 (W.D. Mich. Feb. 8, 2007) (ordering access to a plaintiff's computer systems so as to

⁶ Plaintiff has submitted to this Court an affidavit from her expert, Scott T. Simmons, who appears to be qualified.

⁷ Defendants have submitted to this Court a curriculum *vita*e and two affidavits of their expert, C. Matthew Curtin, who appears to be qualified.

ascertain if “plaintiff accessed [Defendants’] website or a website which advertised [for Defendant], what interaction plaintiff had with such websites and what, if any, information concerning those internet transactions was subsequently deleted”).

Second, Defendants have offered to have their forensic computer expert review with Plaintiff the findings and allow Plaintiff to identify the privileged documents that will then be removed before the information is forwarded to Defendants. Indeed, our sister district court has ordered this exact protocol. *See Thielen*, 2007 U.S. Dist. LEXIS 8998, at *8-9 (court ordered defendant to select forensic expert to mirror image and review plaintiff’s computer hard drive and report findings under confidence to plaintiff’s counsel prior to forwarding it to defendant’s counsel).

Finally, the Court is not heedless of the intrusion copying Plaintiff’s computer systems’ hard drives will cause. In *Playboy Enters. v. Welles*, 60 F. Supp.2d 1050, 1054 (S.D. Cal. 1999), a case upon which Defendants rely, the court stated that the mirror imaging process took approximately four to eight hours for each computer. This amount of time is certainly reasonable to remedy Plaintiff’s failure of his duty to preserve the relevant computer-stored evidence in this action. *See* Fed. R. Civ. P. 37 Advisory Committee’s Note on 2006 Amendments (recognizing the “duty to preserve information because of pending or reasonably anticipated litigation”).

Accordingly, this Court **ORDERS** Plaintiff to permit Defendants’ forensic computer expert to mirror image Plaintiff’s computer systems’ hard drives. Defendants’ expert shall review his findings in confidence with Plaintiff prior to making any findings available to Defendants. Plaintiff shall identify for deletion any information that is irrelevant and create a

specific privilege log of any relevant information for which he claims privilege. The expert shall remove the information claimed as privileged and provide all other information to Defendants.

C. Forensic Computer Experts

It appears to the Court that both of the forensic computer experts presented to it are qualified. In certain situations, courts appoint computer forensic experts to act as officers of the court to help “reduce privacy intrusions and privilege waiver issues during forensic analysis.” Mark E. Borzych, *Avoiding Electronic Discovery Disputes: Practice Questions Answered*, 41 AZ Attorney 36 (January 2005). *See also Thielen*, 2007 U.S. Dist. LEXIS 8998, at *8 (court ordered forensic analysis by third party and accepted that no waiver of privilege occurred). Thus, the two identified computer forensic experts shall serve as officers of this Court.

With regard to the cost of the forensic examinations, at least initially, the parties will bear the costs associated with their chosen expert.

IV. Conclusion

Based on the foregoing, this Court **ORDERS**:

1. Within seven days of the date of this Opinion and Order, Plaintiff’s forensic computer expert shall mirror image both of Plaintiff’s computer systems’ hard drives and Plaintiff shall preserve this mirror image.
2. Plaintiff’s forensic computer expert shall then remove only Plaintiff’s confidential personal information from the mirror image of Plaintiff’s computer systems’ hard drives. Plaintiff’s expert shall provide Defendants with the protocol he utilized to remove the confidential information.
3. Plaintiff shall then provide Defendants’ computer forensic expert access to his

computer systems' hard drives.

4. Defendants' forensic computer expert shall mirror image Plaintiff's computer systems' hard drives in approximately four to eight hours for each system. If the expert finds that this is not enough time, Plaintiff is expected to be reasonable in allowing some additional time. Defendant is expected to be considerate with regard to scheduling times that are less intrusive to Plaintiff and his business.

5. Defendants' expert shall review his findings in confidence with Plaintiff prior to making any findings available to Defendants.

6. Plaintiff shall identify for deletion any information that is irrelevant and create a specific privilege log of any relevant information for which he claims privilege. The computer forensic expert shall remove the information claimed as privileged and provide all other information to Defendants.

7. Defendants' expert shall provide Plaintiff with the protocol he utilized to remove the privileged information.

8. Forensic computer experts C. Matthew Curtin and Scott T. Simmons shall act as officers of this Court. Defendants shall be responsible for remunerating Mr. Curtin and Plaintiff shall be responsible for remunerating Mr. Simmons.

IT IS SO ORDERED.

/s/ Gregory L. Frost
GREGORY L. FROST
UNITED STATES DISTRICT JUDGE