UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF FLORIDA
GAINESVILLE DIVISION

KIM BERRYMAN-DAGES,

Plaintiff, **CASE NO. 1-10cv00177-MP-GRJ**

vs.

CITY OF GAINESVILLE, FLORIDA,

Defendant.
_____/

PLAINTIFF'S RESPONSE IN SUPPORT OF MOTION TO QUASH

Plaintiff supports the motion to quash. The grounds cited in the letter filed by lay witness Nancy Thayer are well-founded. The City's subpoena proposes no safeguards whatsoever. The letter/ motion makes plain the computer likely contains highly-sensitive, possibly privileged data. The City's subpoena will turn this information into a public record. But even if it does not, the City has no legal basis to argue that a lay person not a party to this lawsuit must turn over equipment that will expose all manner of highly-sensitive date that goes far beyond any legitimate need of the City.

The City could not search Plaintiff's computer in such an unfettered manner. The rights of an independent person deserve at least that protection. Under all circumstances, care must be taken to avoid undue intrusiveness resulting from inspecting or testing such systems. Most commonly in situations like this, the parties jointly craft a protocol to be ratified by the Court to provide inspection guidelines. Special consideration is required for inspections of the systems of persons who are not parties. If privileged information is on the computer, its production cannot be compelled.

This Court should quash the subpoena and direct the parties to develop a protocol if any inspection is needed. Thayer is entitled to safeguards. The City fails to provide them.

While there is no universal solution for such circumstances, some basic considerations follow:

Specifying Where To Search

An inspection of a nonlitigant's computer should specify where and for what the requesting party intends to search, or it is likely to be denied. See, e.g., Balfour , 2007 WL 169628, at *3. Examples of possible data repositories in a typical computer include e-mail systems, archive e-mail files (such as Outlook .PST files), portable backup media, home directories, shared files, and backup tapes.

Specifying How The Search Is Conducted

The methodology for data harvesting should be specified in the protocol and must conform to forensic principles for data preservation, including obtaining accurate and complete copies. An accurate copy requires every bit of data on the destination copy to be a true copy of the corresponding bit of data on the source. A complete copy is one where every bit of the source data has been copied to the destination.

An independent forensic expert should be employed to conduct the actual inspection.8 With simpler inspections of hard drives, the expert can perform the actual collection, creating a bit stream image pursuant to standards such as those promulgated by the Department of Justice ("DOJ") or National Institute of Standards and Technology ("NIST"). Hash values, such as those specified by the MD5 standard, can be generated for any given set of data. If so much as a comma in any of the collected documents is subsequently altered, the hash value should no longer match. Through this methodology, the integrity of the collected data can be confirmed.

When dealing with computer systems of private nonparty citizens, specifying who will perform the actual collection is critical. The risk of liability if a computer is damaged during the

inspection - is often too great for the expert to perform the actual extraction. The protocol should obligate the responding party to perform the extraction at the expert's direction and under his or her supervision.

Pre-Inspection Discovery Is Essential

The City should not be permitted to take possession of Thayer's computer simply because it has in-house staff that claim the ability to inspect it. At this point, the City has not deposed Thayer. It does not know where and in what manner relevant data has been stored or, worse, whether testimony may demonstrate conclusively that any relevant information is long gone. That testimony is a critical predicate to inspection. The City's approach is backwards. It has failed to demonstrate that inspection is even justified, much less properly identify what is to be inspected. Nor has it provided reasonable protocol for inspection, for preservation of evidence, or for creation of evidence that would show how the computer has been altered during inspection.

The City Has Failed To Create A Protocol To Protect Nancy Thayer's Privacy Rights And The Privacy Rights Of Those Whose Information Is Stored Thereon

The inspection of electronic information systems raises issues of confidentiality and privacy. Accordingly, even an independent forensic expert should not be allowed to turn collected data over to the requesting party until the responding party has had the opportunity to remove irrelevant and privileged information. An expert can use specialized tools to further refine the collected data to a manageable number of documents to turn over to the requesting party. The protocol might specify what narrowing efforts are expected as these can vary widely in terms of cost, time, and result. A reasonable solution may rely wholly on automatic searches, manual review, or some combination of both. The protocol may also allow the requesting party to play some part in this process by

allowing the expert to reveal certain information, such as volume or metadata, that would allow the requesting party to help the expert narrow the searches used while not revealing any of the contents of the collected documents. The search mechanisms employed, including what search terms are used, may or may not be disclosed to the responding party. After initial culling, the remaining collected data can turned over to the parties for review. A protocol should be developed jointly by the parties here and approved by the Court to specify the format of the data to be provided for review and the contents of any reports that accompany the data. After a specified period of time for review has passed, any non-privileged data, the relevance of which has not been disputed, can be turned over by the expert to the requesting party.

Disputes Over Privilege Or Relevance

The inspection protocol should provide a mechanism for the resolution of disputes as to whether a given document collected during the inspection should be disclosed. With the simpler inspections of hard drives considered by courts to date, some protocols provide for disputed documents to be submitted to the court for in camera review. Other protocols provide for the requesting party to move to compel if it believes the target is improperly withholding responsive or non-privileged documents. Regardless of how the dispute comes before the court, the requesting party is at a strategic disadvantage as it typically does not yet have access to the documents that the expert intends to produce. The protocol can allow for the expert to provide argument to the court as to why a given document falls within the scope of the inspection and should be produced.

CONCLUSION

The discovery process is designed to be extrajudicial, and *normall*y relies upon the responding party to search his records to produce the requested data. In the absence of a strong

showing that the responding party has somehow defaulted in this obligation, a court should not resort to extreme, expensive, or extraordinary means to guarantee compliance. The City's subpoena is such an extreme measure. This Court should quash the subpoena until the parties themselves have had an opportunity to agree on a protocol and, most importantly, an independent expert. For example an independent forensic examiner can be appointed by the court, paid for by one of the parties, or retained jointly by both parties subject to a cost-sharing agreement. But the City's subpoena is overbroad, seeks what is in fact extraordinary access to confidential information, and utterly lacks a framework to assure the proper handling of the Thayer computer. McCurdy Group v. Am. Biomedical Group, Inc., 9 Fed. App'x. 822, 831 (10 th Cir., 2001)("Although [plaintiff] was apparently skeptical that [defendant] produced copies of all relevant and nonprivileged documents from the hard drive(s), that reason alone is not sufficient to warrant such a drastic discovery measure"); Balfour Beatty Rail, Inc. v. Vaccarello, No. 3:06-cv-551-J-20MCR, 2007 WL 169628, at *3 (M.D. Fla., Jan. 18, 2007) (plaintiff had not specifically identified what it was looking for or made any contention that defendant had failed to produce the requested information, therefore inspection would be a "fishing trip"); Calyon v. Mizuho Sec. USA, Inc., No. 07CIV02241RODF, 2007 WL 1468889, at *3 (S.D.N.Y., May 18, 2007)(denying the requested inspection as "Defendants have represented that their expert can and will conduct an exhaustive search of the hard drives for the information Calyon seeks. . . and the Court, at present, has no basis to question this representation)" and Memry Corp. v. Kentucky Oil Tech., N.V., No. C04-03843 RMW, 2007 WL 832937 at *3 (N.D. Cal., Mar. 19, 2007) (denying a request to inspect as the "computer content was [not] intricately related to the very basis of the lawsuit" and any flaws in defendant's production did "not rise to the level of necessitating" inspection). See also Rowe, 205 F.R.D. at 432 (noting that

even with a protective order in place "the disclosure of privileged documents cannot be compelled...")

Respectfully submitted

MARIE A. MATTOX, P. A.

/s/ James Garrity
James Garrity (FBN: 539211)
310 East Bradford Road
Tallahassee, FL 32303
Telephone: (850) 383-4800
Facsimile: (850) 383-4801
ATTORNEYS FOR PLAINTIFF

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a copy of the foregoing has been furnished by CM/ECF service only to all counsel of record this 23rd day of May 2011.

/s/ James Garrity
James Garrity