UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X

LARA CURTO,

Plaintiff,

-against-

MEDICAL WORLD COMMUNICATIONS, INC., ROMAINE PIERSON PUBLISHERS, INC. f/k/a ROMAINE PIERSON ACQUISITION CO., JOHN J. HENNESSY, JAMES GRANATO, DANIEL PERKINS, JAMES KING, ROBERT ISSLER, and EUGENE CONSELYEA,

Defendants.
----------X

MEMORANDUM AND ORDER
03CV6327 (DRH) (MLO)

A P P E A R A N C E S :

For the Plaintiff:
FORCHELLI, CURTO, SCHWARTZ, MINEO, CARLINO & COHN, LLP
330 Old Country Road
Suite 301
Mineola, New York 11501
By: Andrew E. Curto, Esq.

MEYER SUOZZI ENGLISH & KLEIN, P.C.
1505 Kellum Place
Mineola, New York 11501
By: Lois Carter Schlissel, Esq.

For the Defendants Medical World Communications, Inc., Romaine Pierson, Inc., John J. Hennessy, and Robert Issler:
ST. JOHN & WAYNE, L.L.C.
Two Penn Plaza East
Newark, New Jersey 07102
By: James P. Anelli, Esq.

FARRELL FRITZ, P.C.
1320 Reckson Plaza
West Tower
Uniondale, New York 11556
By: John P. McEntee, Esq.

HURLEY, District Judge:

INTRODUCTION

Defendants Medical World Communications, Inc. ("MWC" or the "Company"), Romaine Pierson, Inc., John J. Hennessy, and Robert Issler (collectively, "Defendants") object to the January 18, 2006 Order of Chief Magistrate Judge Michael L. Orenstein which held that Plaintiff Lara Curto ("Plaintiff") had not waived her right to assert the attorney-client privilege and work product immunity concerning documents allegedly retrieved from MWC-owned laptop computers used by Plaintiff during her employment with MWC. For the reasons that follow, Defendants' objections are denied and the January 18, 2006 Order is affirmed in its entirety.

BACKGROUND

I. Factual Background

Plaintiff was employed by MWC from August 1995 to October 24, 2003. MWC has an "E-mail/Computer Privacy Policy," contained within the Employee Handbook, that governs the use of its computer resources. Plaintiff signed an acknowledgment of her receipt and understanding of MWC's Handbook on January 13, 1999, and again on June 5, 2001. The policy provides as follows:

> The computers and computer accounts given to employees are to assist them in the performance of their jobs. Employees should not have an expectation of privacy in anything they create, store, send, or receive on the computer system. The computer system belongs to the company and may be used only for business purposes.
>
> Employees expressly waive any right of privacy in anything they create, store, send, or receive on the computer or through the Internet or any other computer network. Employees consent to allowing personnel of [MWC] to access and review all materials employees create, store, send, or receive on the computer or through the Internet or any computer network. Employees

> understand that [MWC] may use human or automated means to monitor use of computer resources.

(Decl. of Carol Swoboda, dated Jan. 17, 2006, Ex. A ¶ 5.23.2.)

Beginning in May 2002, Plaintiff worked primarily out of her home office in Glenwood Landing, New York. Plaintiff was assigned Company-owned equipment to use in her home, including Company-owned laptop computers. Specifically, Plaintiff was assigned a Company-owned Macintosh ("Mac") laptop computer until May 2003, when she was told that she would be converting to a Dell laptop computer. As a result, Plaintiff had her files from the Mac laptop transferred to the new Dell laptop. Prior to this transfer, Plaintiff deleted her personal files from the Mac laptop, including notes and e-mails she had sent to her attorneys regarding this action. The Mac laptop was then returned to MWC.

On May 15, 2003, Plaintiff was assigned a Dell laptop computer to use in her home office. Plaintiff used the Dell laptop until she was terminated in October 2003, at which time she was instructed to return the Dell laptop to MWC. Before Plaintiff returned it, she again deleted all personal files and written communications to counsel.

Almost two years later, MWC hired a forensic consultant to inspect the Mac and Dell laptop computers that were assigned to Plaintiff. The consultant was able to restore portions of the computer files and e-mails that had been deleted by Plaintiff. On July 1, 2005, MWC produced these restored documents to Plaintiff's counsel. By letter dated July 8, 2005, Plaintiff's counsel asserted that many of these documents were protected from disclosure by the attorney-client privilege and attorney work product immunity. Plaintiff demanded that the files be returned and not disclosed by Defendants.

By letter dated July 11, 2005, Defendants' counsel requested that Plaintiff provide

an explanation as to what documents she was asserting a privilege, the basis of the privilege, when the document was created, and by whom the document was created. After attempts by the parties to resolve this discovery dispute failed, Defendants moved for an order, on August 4, 2005, to determine whether the recovered documents were protected from disclosure.

On September 21, 2005, Magistrate Judge Orenstein held oral argument on the application. He directed Plaintiff to serve and file a privilege log in two weeks and to submit to the Court any documents claimed to be privileged or protected for an in camera inspection. (Sept. 21, 2005 Tr. at 63.) Thereafter, on October 7, 2005, Plaintiff served Defendants with a privilege log and submitted a copy to the Court, together with copies of the allegedly protected documents, which were filed under seal.

In the privilege log, Plaintiff asserted that the following recovered documents should be protected from disclosure under the attorney-client privilege and/or the attorney work product doctrine: (1) a draft memorandum from Plaintiff to John J. Hennessy, MWC's Chief Executive Officer, prepared by Plaintiff and her counsel; (2) a "chronology of events" describing events underlying many of Plaintiff's claims, prepared by Plaintiff and her counsel; (3) drafts of Plaintiff's EEOC complaint prepared by Plaintiff and her counsel; and (4) various e-mails sent amongst Plaintiff and her counsel. Plaintiff is represented in this action by her husband, Andrew Curto, and Lois Carter Schlissel.

After hearing oral argument and reviewing the parties' submissions, Judge Orenstein held, inter alia, that Plaintiff had not waived her right to assert the attorney-client privilege or work product protection as to these documents and directed Defendants to return to Plaintiff all copies thereof. It is this Order, which is discussed in more detail below, which is the

subject of the instant appeal. (*See* Jan. 18, 2006 Tr.)

II. The January 18, 2006 Order

Judge Orenstein began his analysis by noting that the voluntary disclosure of communications protected by the attorney-client privilege generally results in a waiver. (*Id.* at 31 (citations omitted).) "However, the 'inadvertant production of a privileged document does not waive the privilege unless the producing party's conduct was so careless as to suggest that it was not concerned with the [protection] of the asserted privilege." (*Id.* (quoting *SEC v. Cassano*, 189 F.R.D. 83, 85 (S.D.N.Y. 1999) (citation and internal quotation marks omitted.).) Noting that the federal courts have differing approaches in determining the result of a party's inadvertant disclosure, Judge Orenstein found that "the general consensus in this District is that the disclosing party may demonstrate, in appropriate circumstances, that such production does not constitute a waiver of the privilege or work product immunity, and that it is entitled to the return of the mistakenly produced documents." (*Id.* at 32 (citing *Lava Trading, Inc. v. Hartford Fire Ins. Co.*, No. 03 Civ. 7037, 2005 WL 66892, at *2 (S.D.N.Y. Jan. 11, 2005).) Under this approach,

> the courts are called upon to balance four relevant factors: [1] the reasonableness of the precautions taken by the producing party to prevent inadvertant disclosure of privileged documents; [2] the volume of discovery versus the extent of the specific disclosure [at] issue; [3] the length of time taken by the producing party to rectify the disclosure; and [4] the overarching issue of fairness.

(*Id.* at 33 (citing *United States v. Rigas*, 281 F. Supp. 2d 733, 738 (S.D.N.Y. 2003).) Judge Orenstein applied this analysis to the present case and added a further factor or "subfactor":

"whether or not there was enforcement of [any computer usage] policy." (*Id.*)[1]

With regard to this "subfactor" or "subset," Judge Orenstein recognized that the following facts were undisputed: MWC had a computer usage policy which prohibited the personal use of computers, Plaintiff signed the employee handbook containing this policy, and Plaintiff did use the computer for personal use. (*Id.*) But this did "not end the issue" because the lack of enforcement by MWC of its computer usage policy created a "false sense of security" which "lull[ed]" employees into believing that the policy would not be enforced. (*Id.* at 34.) More specifically, he indicated that there were approximately four instances in which MWC monitored the computer use of its employees and that they occurred under very limited circumstances, viz. "when there was a request by either a manager or supervisor or by someone else at [MWC]." (*Id.*) For example, one instance involved an employee who allegedly downloaded pornographic materials, another involved an employee allegedly playing poker on the internet, and finally, another involved an employee allegedly using the computer to conduct an outside business. (*Id.*) Judge Orenstein further noted that at least two of these cases occurred in Chicago and California, respectively, which would not have provided Plaintiff with any notice that the Company monitored computer usage. (*Id.* at 35.)

As for the relevant four factors, Judge Orenstein found that: (1) Plaintiff did take reasonable precautions to prevent inadvertent disclosure in that she sent the e-mails at issue through her personal AOL account which did not go through the Defendants' servers[2] and she

---

[1] Judge Orenstein advised the parties during a previous conference that he would be considering this factor.

[2] Judge Orenstein further noted that several other MWC employees, including its president, had personal AOL accounts on their work computers. (Jan. 18, 2006 Tr. at 36.)

attempted to delete the material before turning in her laptops, (*id.* at 35-36); (2) with regard to the volume of the material inadvertently disclosed compared to the volume of discovery in general, this case involved limited items that were recovered from a computer as opposed to "a tremendous volume of paperwork," (*id.* at 37); (3) "the length of time taken by the plaintiff to rectify the disclosure or at least ask for the documents back was rather immediate, upon notification," (*id.*); and (4) the "overarching issue of fairness" weighed in Plaintiff's favor because clients should be encouraged to provide full disclosure to their attorneys without fear that their disclosure will be invaded, (*id.* at 37-38 (noting recent Second Circuit decision that upheld the attorney-client privilege, "returning the [] privilege back to its former mantle in the law").)[3] After balancing all of these factors, and considering all of the evidence before him, Judge Orenstein concluded that Plaintiff had not waived her right to assert the attorney-client privilege and work product protection with regard to any of the documents retrieved by Defendants from the two laptop computers and directed Defendants to return all such material. (*Id.* at 39.) He then reserved decision as to whether the documents at issue are protected by the attorney-client privilege or work product immunity.[4]

DISCUSSION

I. Standard of Review

This court reviews a magistrate judge's decision regarding non-dispositive

---

[3] *See In re Grand Jury Investigation*, 399 F.3d 527 (2d Cir. 2005).

[4] Defendants have indicated that although Judge Orenstein's Order reserved decision on the issue of work product protection, it is unclear to them whether he also reserved decision on the issue of the attorney-client privilege. (*See* Defs.' Reply at 2-3.) After reviewing the transcript, this Court is of the view that he reserved decision as to both. (*See* Jan. 18, 2006 Tr. at 44.) Thus, as discussed *infra*, any application regarding the determination as to whether these documents are privileged or not should be directed to Judge Orenstein.

pretrial matters under a "clearly erroneous or contrary to law" standard. *See* 28 U.S.C. § 636(b)(1)(A); Fed. R. Civ. P. 72(a). Discovery matters are generally considered non-dispositive of litigation. *See Thomas E. Hoar, Inc. v. Sara Lee Corp.*, 900 F.2d 522, 525 (2d Cir. 1990).

An order is "clearly erroneous" only if a reviewing court, considering the entirety of the evidence, "'is left with the definite and firm conviction that a mistake has been committed'"; an order is "contrary to law" when it "fails to apply or misapplies relevant statutes, case law, or rules of procedure.'" *E.E.O.C. v. First Wireless Group, Inc.*, 225 F.R.D. 404, 405 (E.D.N.Y. 2004) (quoting *Weiss v. La Suisse*, 161 F. Supp. 2d 305, 320-21 (S.D.N.Y. 2001)). This standard is "highly deferential," "imposes a heavy burden on the objecting party," and "only permits reversal where the magistrate judge abused his discretion." *Mitchell v. Century 21 Rustic Realty*, 233 F. Supp. 2d 418, 430 (E.D.N.Y. 2002).

Because it is clear that a magistrate judge is best qualified to "judge the entire atmosphere of the discovery process," *Bogan v. Northwestern Mut. Life Ins. Co.*, 144 F.R.D. 51, 53 (S.D.N.Y. 1992), his discovery-related rulings are entitled to a particular deference. *See Nikkal Indus., Ltd. v. Salton, Inc.*, 689 F. Supp. 187, 189 (S.D.N.Y. 1988) ("Consistently, it has been held that a magistrate's report resolving a discovery discourse between litigants should be afforded substantial deference and be overturned only if found to be an abuse of discretion.").

II. Judge Orenstein's Order Was Neither Clearly Erroneous Nor Contrary to Law

Defendants' argument that Judge Orenstein erred in finding that Plaintiff had not waived her attorney-client privilege and work product protection as to the documents at issue is essentially twofold. First, they argue that Judge Orenstein erred in adopting a factor that he explicitly acknowledged had not been adopted or followed by any other court, (*see* Jan. 18, 2006

Tr. at 3), i.e., whether or not MWC *enforced* its computer usage policy, and that this newly imposed requirement is contrary to well-settled law. Next, they argue that in applying this factor, Judge Orenstein incorrectly concluded that MWC did not enforce its computer usage policy. The Court will address Defendants' contentions in turn.[5]

A. MWC's Enforcement of its Computer Usage Policy

Defendants contend that Judge Orenstein erred in considering MWC's enforcement of its computer usage policy, as no other court has applied this factor. The Court disagrees.

1. Enforcement is a Relevant Consideration

As noted by Defendants, the Second Circuit has not specifically addressed the issue of an employee's expectation of privacy in information placed on an employer's computer system in the context of the attorney-client privilege or work product immunity. Nonetheless, as articulated by Judge Orenstein, courts in this Circuit have consistently adopted a middle of the road approach in determining whether inadvertent disclosure results in waiver. In this regard, courts routinely examine the four factors laid out by Judge Orenstein in analyzing whether "the producing party's conduct was so careless as to suggest that it was not concerned with the [protection] of the asserted privilege." *Cassano*, 189 F.R.D. at 85 (citation and internal

---

[5] In their moving papers, Defendants assert that Judge Orenstein's Order should be reversed for the additional reason that Plaintiff waived any applicable privilege when she failed to timely identify the documents at issue in a privilege log, as required by Local Rule 26.2(a)(2). In response, Plaintiff points out that any such objection on Defendants' behalf is untimely because Judge Orenstein ruled on September 21, 2005 that Plaintiff could have an additional two weeks to submit its log and Defendants' objections were filed on February 1, 2006. Defendants do not address this contention in their reply memorandum, apparently abandoning this objection. In any event, Plaintiff is correct that Defendants' objection in this regard is untimely and, thus, to the extent any such objection is being asserted, it is denied. *See* Fed. R. Civ. P. 72(a).

quotation marks omitted).

After reviewing Judge Orenstein's findings in this regard, this Court concludes that his findings on the four factors were not clearly erroneous or contrary to law. That he added another factor, viz. whether MWC enforced its computer usage policy, does not change this result. Indeed, this additional factor is really just a "subset" of the first factor, i.e., the reasonableness of the precautions taken by Plaintiff to prevent inadvertent disclosure. Moreover, it goes right to the heart of the overriding question which guides the Court's analysis: was Plaintiff's conduct so careless as to suggest that she was not concerned with the protection of the privilege. Accordingly, the Court finds that Judge Orenstein's ruling, which considered the governing four factors as well as the subset of enforcement, was not clearly erroneous or contrary to law.

2. The Expectation of Privacy Cases are not Controlling

Defendants further complain that Judge Orenstein improperly focused on this additional subfactor. In this regard, they contend that "numerous federal courts have held that an employee has no expectation in workplace computer files where [] company guidelines and policy explicitly inform the employee that no expectation of privacy exists." (Defs.' Mem. at 11 (citing *Muick v. Genayre*, 280 F.3d 741, 743 (7th Cir. 2002); *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000); *Thygeson v. Bancorp*, No. CV-03-467, 2004 WL 2066746 (D. Or. Sept. 15, 2004) and *Kelleher v. City of Reading*, No. CIV.A.01-3386, 2002 WL 1067442 (E.D. Pa. May 29, 2002).) All of these cases, however, arise in the context of an employee asserting a right to privacy claim, either under the Fourth Amendment or common law. While these cases may be analogous, they are not controlling as they do not address the confidentiality of

employee's e-mails and personal computer files with regard to the attorney-client privilege or attorney work product immunity.

Moreover, they are all factually distinguishable in an important way – none of these cases involves an employee working from a *home* office. This distinction is particularly significant in *Thygeson*. In that case, the court found that the plaintiff-employee had no reasonable expectation of privacy in files he stored in his personal folder on his computer and in his personal e-mail account because his employer had an "explicit policy banning personal use of office computers and permitting monitoring" *and* because the employer retrieved such information by accessing its own computer network. 2004 WL 2066746, at *21. As to the latter, the court found that the employer "retained the key" to plaintiff's files as it "was able to remotely search [plaintiff's] personal files on the network." *Id.* at *19. Here, Plaintiff's laptops were not connected to MWC's computer server and were not located in MWC's offices; thus, MWC was not able to monitor Plaintiff's activity on her home-based laptops or intercept her e-mails at any time. In fact, in order for MWC to access the documents on Plaintiff's laptops, they would have to be either physically transported to MWC's offices or someone from MWC would have to examine them at Plaintiff's home. When she did have to return her laptop, she deleted all personal files. Thus, it was reasonable for her to believe that the e-mails she sent and the personal documents she stored on her laptops were confidential.

In *Simons*, the policy stated that electronic auditing "shall be implemented" and that "[u]sers shall . . . [u]nderstand [the employer] will periodically audit, inspect, and/or monitor the user's Internet access as deemed appropriate." 206 F.3d at 395-96. The Fourth Circuit found that such language "placed employees on notice that they could not reasonably expect that their

Internet activity would be private." *Id.* at 398. Here, on the other hand, the policy states: "Employees understand that [MWC] *may* use human or automated means to monitor use of computer resources." (Decl. of Carol Swoboda, dated Jan. 17, 2006, Ex. A ¶ 5.23.2 (emphasis added).) Not only is the wording in the policy at issue ambiguous as to whether MWC will conduct audits, because Plaintiff worked at home, as discussed above, any such monitoring would have had to have been preceded by notice to Plaintiff.

The Second Circuit had the opportunity to rule on an expectation of privacy case under the Fourth Amendment in *Leventhal v. Knapek*, 266 F.3d 64, 73 (2d Cir. 2001). In that case, the Second Circuit stated that in determining whether there exists a reasonable expectation of privacy by a public employee in his office computer, "'the context of the employment relation'" should be considered, *id.* at 73 (2d Cir. 2001) (quoting *O'Connor v. Ortega*, 480 U.S. 709, 717 (1987)), "after considering what access other employees or the public had to [the employee's] office," *id.* The Second Circuit found that the plaintiff-employee had a reasonable expectation of privacy in the contents of his office computer as the employer had neither a general practice of monitoring nor a policy governing computer usage. *Id.* at 73-74. Moreover, although the employer had access to all employee-computers, its maintenance thereof was "normally announced." *Id.*

As noted above, the *Leventhal* case is distinguishable because it involves an employee's right to privacy under the Fourth Amendment and does not involve the interplay of this right with the attorney-client privilege or work product immunity. Moreover, as opposed to the present case, in *Leventhal*, there was no applicable policy governing the employee's computer usage. However, to the extent the right to privacy cases are analogous, and to the

extent *Leventhal* considers the employer's access to the employees' computer and whether the employer actually monitored its employee's computer usage, both factors which weigh in the instant Plaintiff's favor, its consideration of these factors is persuasive.

In short, after reviewing the right to privacy cases cited by Defendants, this Court is not of the view that they compel the conclusion that enforcement may not be a relevant factor. Rather, the Court believes it prudent to heed the Supreme Court's instruction in *O'Connor*: "Given the great variety of work environments, . . . the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis." 480 U.S. at 718 . Although the instant case involves the juxtaposition of the right to privacy with the attorney-client privilege and work product immunity, this instruction is relevant nonetheless.

3. The Asia Global Case

The only case cited by the parties which addresses our precise issue, absent the presence of a home office, is *In re Asia Global Crossing, LTD.*, 322 B.R. 247 (S.D.N.Y. Bankr. 2005). As articulated by the court, the issue there was "whether an employee's use of the company e-mail system to communicate with his personal attorney destroys the attorney-client, work product or joint defense privileges in the e-mails." *Id.* at 251. The court began with an analysis of the confidentiality of e-mail communication in general, noting that "[a]lthough e-mail communication, like any other form of communication, carries the risk of unauthorized disclosure, the prevailing view is that lawyers and clients may communicate confidential information through unencrypted e-mail with a reasonable expectation of confidentiality and privacy." 322 B.R at 256 (citations omitted). "Consistent with this trend," New York C.P.L.R. § 4548 provides that "[n]o communication privileged under this article shall lose its privileged

character for the sole reason that it is communicated by electronic means or because persons necessary for the delivery or facilitation of such electronic communication may have access to the content of the communication." N.Y. C.P.L.R. § 4548 (McKinney 1999); *see also Asia Global*, 322 B.R. at 256. "Accordingly, while disagreement exists, the transmission of a privileged communication through unencrypted e-mail does not, without more, destroy the privilege." *Id.* (citation omitted).[6]

Because the *Asia Global* court was unable to locate any decisions discussing the confidentiality of an employee's e-mails in the context of the attorney-client privilege, the court looked to case law pertaining to an "employee's expectation of privacy in his office computer and the company e-mail system" for guidance. *Id.* at 256. The court explained that "[a]s with attorney-client confidentiality, the expectation of privacy has objective and subjective components." *Id.* at 257. Thus, "[f]or Fourth Amendment purposes, the person asserting the right must demonstrate that he has 'a subjective expectation of privacy . . . that society accepts as objectively reasonable.'" *Id.* (quoting *California v. Greenwood*, 486 U.S. 35, 39 (1988)). In making this determination, the *Asia Global* court considered four factors: "(1) does the corporation maintain a policy banning personal or other objectionable use, (2) does the company

---

[6] As noted in the practice commentaries to the statute:

> The new CPLR provision, in effect, constitutes a legislative finding that when the parties to a privileged relationship communicate by e-mail, they have a reasonable expectation of privacy. Some caveats should be noted. The statute provides only that privilege shall not be lost solely because the parties use e-mail. All other aspects of the privilege must be satisfied, including the conventional requirements of confidentiality.

N.Y. C.P.L.R. § 4548, practice commentary.

monitor the use of the employee's computer or e-mail, (3) do third parties have a right of access to the computer or e-mails, and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?" *Id.*

With respect to access, the Court found that anyone who had access to the company's e-mail system could read the employees' e-mails because they were sent over this system and were stored on the company's server. *Id.* at 259. With respect to the other factors, however, "the evidence [was] equivocal regarding the existence or notice of corporate policies banning certain uses or monitoring employee e-mails." *Id.* Therefore, the court was unable to determine as a matter of law whether the employees' use of the company e-mail system to communicate with their attorneys eliminated any existing attorney-client privilege. *Id.* at 261.

Although the court in *Asia Global* did not explicitly discuss whether the employer actually monitored employees' computer usage, other than to acknowledge that the employees claimed that there was no such monitoring, it did recognize enforcement as a factor to be considered. Accordingly, the *Asia Global* case, though not binding, lends further support for Judge Orenstein's consideration of this factor in his analysis.

4. Conclusion

In sum, the Court finds that Judge Orenstein's consideration of whether MWC enforced its computer usage policy was not clearly erroneous or contrary to law. Although Defendants contend that "the new enforcement requirement created by Magistrate Judge Orenstein" may require employers to "read all email messages sent or received by employees," "review every internet web site visited by an employee," and search employee's personal computer documents so as to ensure that they don't lose their right to enforce computer usage

policies, (Defs.' Mem. at 6), Defendants misconstrue Judge Orenstein's ruling. In considering whether MWC enforced its policy, Judge Orenstein in no way indicated that this factor was dispositive. In fact, he himself characterized it as a "sub-factor" to be examined, along with the other four relevant factors, which he considered at length.

Moreover, Defendants' suggestion that "if this new requirement is adopted, employees who use company computers to view pornography, to send and receive sexually or racially explicit materials, or to send company trade secrets and confidential information, could claim an expectation of privacy so long as a subjective determination was thereafter made that the employer did not regularly monitor employee computer usage" is equally off-point. The Court's holding is limited to the question of whether an employee's personal use of a company-owned computer in her home waives any applicable attorney-client privilege or work product immunity that may attach to the employee's computer files and/or e-mails. It does not purport to address an employee's right to privacy in an office computer in general. Accordingly, Defendants' claimed "policy" concerns are unfounded.

B. MWC's Enforcement of its Computer Usage Policy

Defendants also contend that Judge Orenstein erred in finding that MWC did not enforce its computer usage policy. Judge Orenstein found that in light of the few instances of actual monitoring by MWC and the surrounding circumstances thereof, together with the fact that many MWC employees had personal e-mail accounts at work, including the President, MWC employees were lulled into a "false sense of security" regarding their personal use of company-owned computers. (Jan. 18, 2006 Tr. at 34- 37.) Thus, he concluded that this "factor really balances overwhelmingly in favor of" Plaintiff. (*See id.* at 37.) After careful

consideration of the record as a whole, the Court finds Judge Orenstein's ruling in this regard was not clearly erroneous or contrary to law.

CONCLUSION

For the foregoing reasons, the Court finds that Judge Orenstein's January 18, 2006 Order was not clearly erroneous or contrary to law. Accordingly, Defendants' objections are denied and the January 18, 2006 Order is affirmed. Any applications regarding whether the documents at issue are protected by the attorney-client privilege or work product immunity shall be directed to Judge Orenstein forthwith.

SO ORDERED.

Dated: Central Islip, New York
May 15, 2006

/s
Denis R. Hurley
United States District Judge