Front, Inc. v Khalil

2013 NY Slip Op 31613(U)

July 9, 2013

Sup Ct, New York County

Docket Number: 111597/11

Judge: Donna M. Mills

Republished from New York State Unified Court System's E-Courts Service.
Search E-Courts (http://www.nycourts.gov/ecourts) for any additional information on this case.

This opinion is uncorrected and not selected for official publication.

SCANNED ON 7/22/2013

[* 1]

SUPREME COURT OF THE STATE OF NEW YORK— NEW YORK COUNTY

PRESENT : DONNA M. MILLS PART 58
Justice

FRONT, INC.,

Plaintiff,

-v-

PHILIP KHALIL, JAMES O'CALLAGHAN, and ECKERSLEY O'CALLAGHAN STRUCTURAL DESIGN,

Defendants.

INDEX NO. 111597/11

MOTION DATE

MOTION SEQ. NO. 04

MOTION CAL NO.

The following papers, numbered 1 to _____ were read on this motion for _____.

PAPERS NUMBERED

Notice of Motion/Order to Show Cause-Affidavits– Exhibits.... 1-5

Answering Affidavits– Exhibits

Replying Affidavits

CROSS-MOTION: ✓ YES ____ NO

FILED
JUL 22 2013
NEW YORK
COUNTY CLERK'S OFFICE

Upon the foregoing papers, it is ordered that this motion is:

DECIDED IN ACCORDANCE WITH ATTACHED ORDER.

Dated: 7/9/13

DONNA M. MILLS, J.S.C.

Check one: ____ FINAL DISPOSITION ✓ NON-FINAL DISPOSITION

[* 2]

FILED

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK : IAS PART 58

----------X

FRONT, INC.,

Plaintiff,

-against- Index No. 111597/11

PHILIP KHALIL, JAMES O'CALLAGHAN, and ECKERSLEY O'CALLAGHAN STRUCTURAL DESIGN,

Defendants.

----------X

PHILIP KHALIL,

Third-Party Plaintiff,

-against-

JEFFREY A. KIMMEL and MEISTER SEELIG & FEIN LLP,

Third-Party Defendants.

----------X

PHILIP KHALIL,

Second Third-Party Plaintiff,

-against-

MARC SIMMONS,

Second Third-Party Defendant.

----------X

FILED
JUL 22 2013
NEW YORK
COUNTY CLERK'S OFFICE

DONNA MILLS, J.:

Second third-party defendant, Marc Simmons (Simmons), moves to dismiss the second third-party complaint (Khalil complaint). Defendant/second third-party plaintiff, Philip Khalil (Khalil), opposes the motion to dismiss and cross-moves for an order suppressing from evidence all emails and documentary evidence

accessed from Khalil's personal and business email accounts by plaintiff Front, Inc. (Front) and Simmons.

This series of actions arises from an employment dispute between Front and its former employee, Khalil. In the underlying complaint Front alleges that Khalil worked together with defendants from the United Kingdom to use Front's confidential and proprietary information to divert work from Front. The underlying complaint further alleges that three days after Khalil had tendered his written resignation from Front, the company's network engineer, Alex Yau, noticed an external hard drive storage device attached to Khalil's office computer. Yau notified Simmons, and the next morning Simmons discovered that Khalil had downloaded files from the office computer, including files containing Front's allegedly confidential and propriety information.

The Khalil complaint alleges that, while Khalil was still employed by Front, Simmons, a partner of Front, accessed and confiscated an external hard drive belonging to Khalil, that contained Khalil's emails and confidential information. The Khalil complaint further alleges that Front did not have a policy prohibiting the use of company computers for the purpose of personal email activity and did not inform employees that their computers would be monitored. It further alleges that Khalil had exclusive use of his office computer and did not share it with

other employees, and that he had a reasonable expectation of privacy with respect to the electronic data stored on his computer and his external hard drive. Finally the Khalil complaint alleges that Simmons acted with intent and malice, in retaliation for his decision to resign from the company and start a new business in New York which Simmons considered a competitor.

The Khalil complaint asserts four causes of action: 1) damages for violation of the Stored Communications Act (SCA), 18 USC § 2707; 2) declaratory and injunctive relief, pursuant to the SCA, including but not limited to preclusion of the use of Khalil's emails in this litigation; 3) conversion; and 4) declaratory and injunctive relief including but not limited to return of Khalil's emails and confidential information, preclusion of the use of that information and destruction of any copies.

Motion to Dismiss

Moving to dismiss the first and second causes of action, Simmons argues that Front's action of accessing and retaining Khalil's external hard drive does not constitute a violation of the SCA, which provides that a person violates the SCA who

> "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
> (2) intentionally exceeds an authorization to access that facility;
> and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system...."

[* 6]

18 USC §.2701 (a).

The SCA further provides:

"(a) Cause of action.--Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

"b) Relief.--In a civil action under this section, appropriate relief includes--

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c); and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

"(c) Damages.--The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000. If the violation is willful or intentional, the court may assess punitive damages. In the case of a successful action to enforce liability under this section, the court may assess the costs of the action, together with reasonable attorney fees determined by the court."

18 USC § 2707.

In support of his motion to dismiss, Simmons submits the affidavit of Alex Yau, Front's network engineer. Yau states that on the evening of March 23, 2011, he noticed an external hard drive device connected to the Front computer assigned to Khalil. The next morning Yau notified Simmons, and later that morning

Yau, Front director, Bruce Nichol, and Khalil viewed the contents of the external hard drive. According to Yau, in addition to some of Khalil's personal information, the device contained hundreds of thousands of files of Front's information. Yau states that he was present and heard a discussion between Nichol and Khalil in which they agreed that Yau would transfer Khalil's information to another external hard drive and give that device to Khalil. Yau states that he did copy the information to a second external hard drive as agreed to by Nichol and Khalil, and that later that day he gave the second device to Khalil.

Yau further states that:

> "17. The copies of Khalil's emails that were stored on Front's computer system were "dead copies," meaning there was no live activity and they were simply stored on the hard drive of Front's server.
> "18. The dead emails stored on Front's computer system were from an Exchange email account, which Front provided to Khalil for business use, and sent emails from a Gmail account Khalil had apparently set up himself.
> "19. No one at Front accessed live data to retrieve Khalil's emails from either account. Rather, Khalil caused the emails Front subsequently reviewed to be saved on Front's hard drive. Khalil ran the emails from the personal account through Front's Outlook software, which resulted in Khalil saving a copy of sent items through Gmail into the Front Exchange account and Front's Exchange Server backup systems. The default primary account that Front assigned to Khalil in the Outlook software was the Front-provided Exchange account pkhalil@frontinc.com. A user, such as Khalil, can configure the Outlook software to interface with secondary accounts, such as Gmail. The default behavior of Outlook is to copy all items sent by Outlook into the primary account, including emails sent through secondary email account services. Khalil saved the emails from the personal account onto Front's

> computer system in its entirety, including information stored on the hard drive of Front's server."

Aff of Alex Yau, ¶¶ 17-19.

Khalil does not contest Yau's statement that Khalil had stored copies of his personal emails on Front's computer system, Yau's explanation of how Front's computer storage system works, or that the external hard drive contained what appeared to be Khalil's personal information, as well as hundreds of thousands of files of Front's information. In fact, Khalil does not directly address Yau's affidavit at all. Rather, Khalil contends that the allegations in his second third-party complaint must be deemed true that "Mr. Simmons intercepted emails from my open Gmail account, that through 'unauthorized' use of my office computer, that he accessed my 'active Outlook account,' through which he *intercepted* 'emails being sent and received through Gmail and other accounts.'" Aff of Philip Khalil, ¶ 24 (emphasis supplied). In support of his contention, Khalil points to copies of certain emails annexed to an affidavit of Simmons submitted by Front in an earlier stage of this litigation, which indicate that those emails were sent from Khalil's personal Gmail account, claiming that the emails show that Simmons was accessing live data, not old emails stored on a hard drive.

Although it is true that on a motion to dismiss, the allegations in a complaint must be accepted as true, and the allegations must be construed in a light most favorable to the

plaintiff, this is not the case where affidavits and evidentiary matter negate the essential facts alleged. *Biondi v Beekman Hill House Apt. Corp.*, 257 AD2d 76, 81 (1st Dept 1999), *affd* 94 NY2d 659 (2000).

Moreover, Khalil's statement in his affidavit is not an accurate characterization of what is alleged in his complaint. The Khalil complaint itself repeatedly alleges that Simmons "accessed" Khalil's "external hard drive and reviewed its contents" and "accessed personal and confidential information contained on [his] office computer." *See* Khalil complaint, ¶¶ 5 and 6. His complaint does not allege that Front or Simmons directly accessed his Gmail account (as opposed to viewing copies of emails that he saved on his office computer) and he does not employ the word "intercepted," which might imply that Simmons directly accessed Khalil's personal email account on-line. Khalil's attorney similarly adds the word "intercepted" to his restatement of the allegations of the complaint when that word was not contained in the complaint, in an apparent effort to suggest that Khalil's Gmail account was directly accessed by Simmons. Affirmation of Neil G. Marantz, ¶ 31. This belated and somewhat misleading use of the word "intercepted" by Khalil and his counsel is insufficient to overcome the allegations of his own complaint. Nor does it overcome Yau's sworn statement that the emails and other information inspected by Yau, Nichol and

Khalil on Khalil's external hard drive, had been saved by Khalil on Front's computer hard drive and then downloaded to the external hard drive, and were not obtained by Front by logging on to Khalil's personal email account via the internet.

Moreover, the specific emails on which Khalil relies in his opposition to Simmons's motion, to prove that Front accessed his personal email account, are dated January 24, 2011, November 16, 2010, and March 21, 2011, and, thus, were sent or received prior to the date when Yau noticed the external hard drive attached to Khalil's office computer which was being used to copy documents from that computer. The presence of those emails on Khalil's external hard drive is, therefore, consistent with Yau's explanation that Khalil had saved, on his office computer, emails sent and received by him, and that no live communication on his Gmail account was accessed by Front, and does not establish that his personal Gmail account was accessed.

Though the language used in discussing computer systems can be a bit confusing to lay persons, the case of *Pure Power Boot Camp v Warrior Fitness Boot Camp* (*Pure Power*)(587 F Supp 2d 548 [SD NY 2008]), relied on by Khalil, is useful to understand what the SCA is and is not designed to prevent. In that case, the employer directly accessed the former employee's personal Hotmail accounts by using the employee's user name and password that he had stored on his work computer and had allegedly given to

another former co-worker. In discussing the SCA the court explained that "[t]he Act 'aims to prevent hackers from obtaining, altering or destroying certain stored electronic communications.'" *Id.* at 555 (citations omitted). The court further explained that the majority of courts that have addressed the issue of electronic storage have determined that "e-mail stored on an electronic communication service provider's systems after it has been delivered, as opposed to e-mail stored on a personal computer, is a stored communication subject to the SCA." *Id.* The court stated:

> "It is important to note from the outset, that this is not a situation in which an employer is attempting to use e-mails obtained from the employer's own computers or systems. Rather, the e-mails at issue here were stored and accessed directly from accounts maintained by outside electronic communication service providers."

Id. at 554. *See also Hilderman v Enea TekSci, Inc.*, 551 F Supp 2d 1183, 1204-1205 (SD Cal 2008)(emails stored on a hard drive do not constitute "electronic storage" for the purposes of the SCA).

As the court explained in *In re DoubleClick Inc. Privacy Litigation* (154 F Supp 2d 497, 511 n 20 [SD NY 2001]), examples of electronic communication service providers (in the year 2001 when the case was decided) are America Online, Juno and UUNET. Gmail, would presumably also fall within that category. As noted above, an employer's computer hard drive (as well as the employer's own computer system) does not constitute an electronic communication service provider, and, thus, is not the focus of

the SCA.

Unlike the situation in *Pure Power,* there is no evidence here, other than Khalil's unsupported assertion in his affidavit, that Simmons or any other Front employee directly access his personal email account maintained by Gmail or any other outside electronic communication service provider. Rather, as the Khalil complaint alleges, Simmons accessed Khalil's external hard drive and information contained on his office computer, which, as Yau explained, included copies of emails which Khalil saved on the computer supplied by Front, and then transferred to his own external hard drive.

As the courts in *Pure Power* and *DoubleClick* indicated, neither an office computer hard drive nor an external hard drive constitute a "facility through which an electronic communication service is provided" (18 USC § 2701 [a] [1]), for the purposes of the SCA. And as the *Pure Power* court also indicated, accessing copies of emails stored by Khalil on his office computer and downloaded by him to his external hard drive does not constitute a violation of the SCA. Thus, the court need not reach Simmons's argument that he was authorized to access the Front hard drive. Simmons's motion to dismiss the first and second causes of action against him is, therefore, granted.

Simmons also moves to dismiss the third cause of action for conversion, arguing that the cause of action for conversion was

not properly pled.

> "A conversion occurs when a party, 'intentionally and without authority, assumes or exercises control over personal property belonging to someone else, interfering with that person's right of possession' (*Colavito v New York Organ Donor Network, Inc.*, 8 NY3d 43, 49-50 [2006]). 'Two key elements of conversion are (1) the plaintiff's possessory right or interest in the property and (2) the defendant's dominion over the property or interference with it, in derogation of plaintiff's rights.' (*id.* at 49-50 ... [citation omitted])."

Lynch v. City of New York, --- AD3d ----, 965 NYS2d 441, 446 (1st Dept 2013).

Simmons argues that Khalil failed to plead the two elements of conversion set forth above, and merely alleged that by confiscating the external hard drive that belonged to him, Simmons had committed conversion. The court, however, agrees with Khalil, that his allegations that, without authorization,[1] Simmons accessed his external hard drive and reviewed its contents which contained personal emails, confiscated the external hard drive and exercised dominion and control over that hard drive and the information, satisfied the pleading standards set forth above. In any case, evidence of the full contents of the external hard drive is not yet before the court.

Citing *Pella Realty v Commissioner of Fin.* (5 AD3d 278, 279 [1st Dept 2004]), Simmons also argues that a legal entitlement to

---

[1] Yau's unsupported assertion that Simmons had the authority to access Front's computer system in its entirety is insufficient to overcome Khalil's allegation.

the property is essential to a cause of action for conversion. Simmons contends that Khalil failed to allege that he had a legal right to retain the external hard drive, and that if, as Front alleged in its original complaint against Khalil, the external hard drive contained Front's confidential information, then Khalil would likely not have a legal right to retain it. However, even if Khalil might not have had a right to retain Front's documents, he would presumably have a possessory right to his own personal documents and the external hard drive, though with Front's documents removed.[2]

Citing *Koeniges v Woodward* (183 Misc 2d 347 [Civ Ct, NY County 2000]), Simmons further contends that to survive a motion to dismiss, plaintiff must show that he has suffered compensatory damages. However, the decision in *Koeniges* followed both discovery and trial, and merely indicates that, there, the plaintiff had failed to prove the damages he was seeking, and not that it was necessary to plead specific damages to state a cause of action for conversion.

Furthermore, here, in addition to his claim for damages, pursuant to his fourth cause of action, Khalil is also seeking injunctive relief in the form of return of his emails and other allegedly confidential information, preclusion of their use by

---

[2] The court notes, but does not speculate about the reason why the relief requested by Khalil in his complaint does not include return of the actual external hard drive.

Simmons in this litigation, or in any other way, and destruction of all copies of the information, and return of his external hard drive. Although the court has seen copies of a limited number of Khalil's emails that were obtained by Front from Khalil's external hard drive, the totality of Khalil's documents obtained by Front when it confiscated Khalil's external hard drive is not yet known. It is similarly unclear whether any justification exists for Front to retain copies of those yet-unknown documents. Thus, at this stage of the litigation, Simmons's motion with respect to the third and fourth causes of action must be denied.

Cross Motion to Suppress

Khalil cross-moves to suppress from evidence all emails and documentary evidence accessed from his personal and business email accounts by Front and Simmons.

To the extent that Khalil seeks to suppress his emails based upon the SCA, the court has already concluded that the information was not obtained in violation of the SCA.

Khalil also relies on his right of privacy in his effort to suppress the emails obtained by Front and Simmons. Khalil contends, and Front has not contested, that the company had no policy barring the use of his office computer for personal email activity. Citing *Scott v Beth Israel Med. Ctr. Inc.* (17 Misc 3d 934 [Sup Ct, NY County 2007]), Khalil argues that he, therefore,

had a reasonable expectation of privacy with respect to any information stored on his computer, and that his personal communications must remain out of his employer's reach. Khalil quotes the decision in *In re Asia Global Crossing, Ltd.* (322 BR 247, 257 (Bankr, SD NY 2005) as setting forth the factors to be considered with respect to an employee's expectation of privacy with respect to his emails:

> "In general, a court should consider four factors: (1) does the corporation maintain a policy banning personal or other objectionable use, (2) does the company 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?"

The court notes that in both *Scott* and *Asia Global Crossing*, the question of privacy of the emails at issue arose where those emails involved attorney-client communications, and the court was considering whether transmission of those communications via email would result in a waiver of the attorney-client privilege. Here, of course, there is no allegation that such privileged communications were involved - rather the communications were personal in nature.

Most of the cases reviewed by the court in *Asia Global Crossing* in its discussion of an employee's expectation of privacy in his computer files and emails involved situations where the employer did in fact have an articulated policy prohibiting or limiting personal use of the office computer and,

thus, no reasonable expectation of privacy was found. Some of the cases examined by the court in *Asia Global Crossing* are instructive, however, in determining how the emails and other allegedly personal documents should be treated here, where Front apparently failed to articulate a policy preventing the use of office computers for personal use. For example, in the case of *Leventhal v Knapek* (266 F3d 64 [2d Cir 2001]), where the New York State Department of Transportation (DOT) searched the computer of its employee, the agency did not maintain a practice of searching office computers and had not placed the employee on notice that he should have no expectation of privacy with respect to his computer, and the anti-theft policy maintained by the agency did not prohibit the employee from merely storing personal materials on his office computer. The Court, therefore, concluded that the employee did have an expectation of privacy with respect to his computer. Nonetheless the Court explained that, even where there is an expectation of privacy, that expectation may be overcome where "'there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct.'" *Leventhal v Knapek*, 266 F3d at 75 (citation omitted). The Court stated that in the circumstances of that case, although the employee had "some expectation of privacy" (*id.*), DOT's search of the computer was justified because the agency had reasonable grounds to believe that the

searches of his computer would uncover evidence of misconduct and the scope of the searches was not "'excessivly intrusive in light of the nature of the misconduct.'" *Id.* at 76 (citation omitted); *see also Smyth v Pillsbury Co.*, 914 F Supp 97, 101 (ED Pa 1996) (any reasonable expectation of privacy in the contents of email sent over the employer's email system is outweighed by the company's interest in preventing inappropriate, unprofessional or illegal conduct).

Here, there is no allegation of regular surveillance of Khalil's computer by Front. Rather, the emails which Khalil seeks to suppress were found by Front because only a few days after Khalil tendered his written resignation, it was discovered that he was downloading documents from his office computer to an external hard drive. Then, with Khalil present, the contents of that hard drive was inspected by Front. Thus, as in *Leventhal*, even if Khalil may have had some expectation of privacy with respect to his computer, it was not unreasonable for his employer to examine the contents of the external hard drive to determine whether any of Front's documents were being downloaded by its employee, who had just tendered his resignation. It is undisputed that some emails which were originally sent or received through Khalil's personal Gmail account were found, as well as others sent or received through Front's work email account that were related to work Khalil was performing for

another employer while he was employed by Front, at least raising a question of work-related misconduct. According to Yau, and undisputed by Khalil, large numbers of Front's documents were also found. Examining the totality of the external hard drive cannot be said to be excessively intrusive in light of what was found there.

Khalil also seeks to suppress the emails based upon the rulings in *Pure Power* and *Forward v Foschi* (27 Misc 3d 1224[A], 2010 NY Slip Op 50876[U] [Sup Ct, Westchester County 2010]). In both cases, however, the information was admittedly accessed by the employer by logging directly on to the employee, or former employee's personal email account via the internet. Additionally, in *Forward*, the information that was obtained was protected by the attorney-client privilege, and was sent by plaintiff to his counsel. In *Forward*, suppressing the emails as evidence was considered a less drastic remedy than that originally requested by defendant - disqualification of plaintiff's counsel. In *Pure Power*, although the emails were suppressed, the court ruled that they could be used for impeachment purposes if the defendant opened the door.

Here, as previously noted, and unlike both *Pure Power* and *Forward*, there is no evidence that Front or Simmons actually accessed Khalil's personal email account. Rather, both the allegations in the Khalil complaint and Yau's sworn statements

indicate that, to the extent that copies of Khalil's personal emails were accessed, that was accomplished by viewing copies he had saved on the hard drive of his office computer and then downloaded to an external hard drive.

Given that it appears that Front had no policy prohibiting the use of its computers to access personal email accounts, had the copies of Khalil's emails been obtained as a result of routine surveillance by Front of Khalil's computer, the question of suppression of those emails might have had a different outcome. Here, however, the emails were found by Front when its network engineer noticed that documents were being copied to an external hard drive, and the contents of the hard drive were examined, with Khalil present. Thus, the court concludes that under the circumstances, any expectation of privacy Khalil might otherwise have had that would have justified the suppression of the emails stored on his computer was overcome when he downloaded those emails, along with Front documents, to his external hard drive.

Accordingly, it is hereby

ORDERED that the motion to dismiss of second third-party defendant Marc Simmons is granted to the extent that the first and second causes of action of the second third-party complaint are dismissed, and it is otherwise denied; and it is further

ORDERED that the cross motion of defendant/second third-

party plaintiff Philip Khalil to suppress from evidence all emails and documentary evidence obtained from Khalil's personal and business email accounts is hereby denied.

Dated: 7/9/13

ENTER:

J.S.C.

DONNA M. MILLS, J.S.C.

FILED
JUL 22 2013
NEW YORK
COUNTY CLERK'S OFFICE