Rad v IAC/Interactivecorp
2020 NY Slip Op 30410(U)
February 11, 2020
Supreme Court, New York County
Docket Number: 654038/2018
Judge: Saliann Scarpulla

SUPREME COURT OF THE STATE OF NEW YORK
NEW YORK COUNTY

PRESENT: **HON. SALIANN SCARPULLA** **PART** **IAS MOTION 39EFM**

Justice

----------X

SEAN RAD, PAUL CAFARDO, GARETH JOHNSON, ALEXA MATEEN, JUSTIN MATEEN, RYAN OGLE,

Plaintiff,

- v -

IAC/INTERACTIVECORP, MATCH GROUP, INC., MATCH GROUP, LLC,

Defendant.

----------X

INDEX NO. 654038/2018

MOTION DATE N/A

MOTION SEQ. NO. 014

DECISION + ORDER ON MOTION

The following e-filed documents, listed by NYSCEF document number (Motion 014) 586, 587, 588, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 600, 601, 602, 604, 631

were read on this motion to/for DISCOVERY.

Plaintiffs Sean Rad ("Rad"), Justin Mateen ("Mateen") and nonparty Rosette Pambakian ("Pambakian") (together "Movants") move for a protective order to prevent the disclosure of their allegedly privileged and confidential communications with their personal attorneys (the "allegedly privileged communications"), which they transmitted on Tinder email systems while they were employed at Tinder. Defendants IAC Interactive Corp. ("IAC"), Match Group, Inc. and Match Group, LLC ("Match") (together "Defendants") oppose the application.

Background

Movants are former top executives of Tinder, a well-known dating application. At all relevant times, Tinder was owned by Match, and IAC was the majority owner of Match. Rad founded Tinder in February 2012 and served as CEO at various points from 2012 to 2016; he left Tinder in September 2017. Mateen founded Tinder and served as

its Chief Marketing Officer from approximately February 2012 to September 2014 and was an advisor from 2014 to 2017. Pambakian was affiliated with Tinder as of 2012, and joined Tinder full-time in March 2014, serving as its Vice President of Marketing and Communications until December 2018.

While they were at Tinder, Movants sent and received the allegedly privileged communications from their Tinder email accounts.[1] Because the allegedly privileged communications reside on Defendants' electronic communications systems, Defendants are in possession of them, and Movants move for an order clawing them back and preventing Defendants from using them in this litigation. Movants argue that they had a reasonable expectation of privacy as to the allegedly privileged communications and have therefore not waived the attorney-client privilege with respect to them. Defendants argue that, having used their Tinder email accounts to send and receive the allegedly privileged communications, with notice that Defendants' communications systems were not private and could be monitored, Movants had no reasonable expectation of privacy as to the allegedly privileged communications and have waived the attorney-client privilege as to them.

Discussion

In *Peerenboom v. Marvel Entertainment, LLC,* the Appellate Division, First Department endorsed application of the four factors set forth in *In Re Asia Global*

[1] At oral argument Movants represented that there are, in total, approximately one hundred and thirty- five allegedly privileged communications that were sent over a six-year period. *See* NYSCEF Doc. No. 631, p. 95.

Crossing, Ltd, 332 BR 247 (Bankr. SDNY 2005) to determine whether a party waives attorney-client privilege by sending the communications through its employer's email system. *Peerenboom v. Marvel Entertainment, LLC,* 148 AD3d 531(1st Dep't 2017). The four factors are:

> (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?

In re Asia Global Crossing Ltd., 332 BR at 257 (citations omitted); *see also Peerenboom,* 148 AD3d at 531; *Miller v. Zara USA,* 151 AD3d 462 (1st Dep't 2017).

Defendants have submitted electronic communication policies from Tinder, Match and IAC all showing that, while Defendants did not ban personal use of Defendants' electronic communications systems, Defendants did strictly limit personal use, expressly told employees that they should have no expectation of privacy while using Defendants' electronic communication systems, and Defendants reserved the right to monitor employees' use of the electronic communications systems. The parties also submit affidavits showing that Defendants widely disseminated their electronic communications policies so that employees would have actual or constructive notice thereof.

Thus, the Tinder electronic communication policy in place during relevant periods provided:

> Tinder, Inc. employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.
>
> Tinder, Inc. may monitor and read all email messages without prior notice.

* * * * *

> Users are responsible for exercising good judgment regarding the reasonable use of equipment for personal use. Any personal use should not unreasonably place any system in jeopardy of compromise or conflict with any HR policies . . . For security and maintenance purposes, authorized individuals within Tinder, Inc. may monitor any and all equipment, systems and network traffic, including decrypting traffic when necessary, without further notification to the user. . . Tinder, Inc. reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

(Trummer Aff. and Exhs., NYSCEF Doc. NO. 589).

Similarly, IAC's electronic communication policy during the relevant time periods provides, among other things, that:

> The Company Systems and all communications created, received, stored, or transmitted on, by, or through the Company Systems are and will at all times remain the property of IAC. Accordingly, the Company Systems should be used for Company purposes only. While the Company understands that some personal use may occur from time to time, such use should be kept to a minimum.
>
> * * * * *
>
> IAC reserves the right to inspect, examine, and monitor the use of the Company Systems at any time, without notice, and for any reason, including the enforcement of this and other IAC policies. Further, IAC reserves the right to review and disclose employees' electronic communications in connection with potential and pending lawsuits, investigations, and other proceedings. Accordingly, no employee should have any expectation of privacy as to his or her use of the Company Systems.

(Hill Aff. and Exhs., NYSCEF Doc. No. 590; *see also* Ferguson Aff., NYSCEF Doc. No. 591 (confirming that all IAC employees were informed of the foregoing at all relevant times)).

In addition, in 2016 IAC "consolidated a number of individual policies . . . into an employee handbook (the 'IAC Employee Handbook') which was posted on IAC

Connect." Chun Aff. ¶ 2 (NYSCEF Doc. No. 592). The first line of the IAC Employee Handbook section concerning "Information Security and Use of Computer Systems" states, in bright red letters:

> Let's be clear, you should have absolutely no expectation of privacy with regard to ANYTHING you do on Company computers or systems.

Finally, Match's electronic communication policy during the relevant time period stated:

> Match reserves the right to inspect, examine, and monitor the use of all of its computers, computer networks, electronic mail, telephone systems (including voicemail), and other electronic communication system s at any time and without notice to the extent necessary or appropriate to ensure that electronic media and services are being used in compliance with the law and with this and any other applicable Match policies. No employee should have any expectation of privacy as to his or her usage of any of these Match systems or the content of any communications thereon.

(Chiles Aff. and Exhs., NYSCEF Doc. No. 593).

Defendants' electronic communication policies are substantially the same as those in *Peerenboom* and *Miller*. And, as in those cases, application of the four *Asia Global* factors here shows that Movants could not have had a reasonable expectation that their communications with their personal attorneys, sent and received on Defendants' electronic communications systems, would be confidential. First and foremost, every policy of Tinder, Match and IAC plainly states that employees should not have any expectation of privacy with respect to communications sent and received on Defendants' electronic communications systems. Further, Defendants each reserved the right to monitor and review all electronic communications. And, while none of Defendants strictly prohibited personal electronic communications, Defendants made clear that

personal electronic communication should be minimal and should conform to Defendants' electronic communications policies.

Significantly, Movants, who were all high-level, key Tinder employees, do not deny that that they had access to Defendants' electronic communications policies, all of which plainly stated that Defendants had the right to monitor and review all electronic communications on Defendants' electronic communication systems.[2] Nor do Movants deny that they knew that their electronic communications were not private and could be reviewed and monitored. In fact, Defendants submit email and text messages from and to Movants which show their understanding that electronic communications sent and received on Defendants' electronic communications systems were not private. *See* Werbelow Aff. and Exhs., NYSCEF Doc. Nos. 596-601.

Considering Defendants' express electronic communication policies, and the evidence submitted evidencing that Movants understood that their electronic communications were not private, I find that Movants have not met their burden of showing that they had a reasonable expectation of privacy in their Tinder electronic communications with their personal attorneys. *See Peerenboom v. Marvel Entertainment*, 148 AD3D 531; *Miller v. Zara USA*, 151 AD3d 462.[3] Accordingly, I

---

[2] Defendants submit written acknowledgements from Movants showing that they had access to one or more of Defendants' employment policies, including policies concerning electronic communications, during the relevant time period. (Chiles Aff. and Exhs., NYSCEF Doc. No. 593).

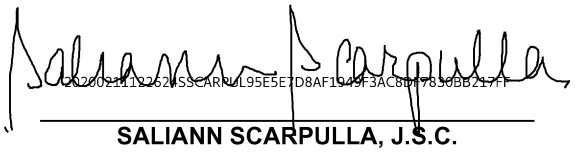
[3] The cases Movants cite are nonbinding federal cases, mostly from non-New York jurisdictions, and are distinguishable.

deny the motion for a protective order. I note that Movants have not claimed work product or any other privilege with respect to the allegedly privileged communications, thus I have not considered the application of any other privilege.

In accordance with the foregoing, it is

ORDERED that the motion of plaintiffs Sean Rad, Justin Mateen and nonparty Rosette Pambakian for a protective order, pursuant to CPLR 3103 and the Court's inherent authority, to prevent the disclosure of their allegedly privileged and confidential communications with their personal attorneys transmitted on Tinder's electronic communications system, is denied.

This constitutes the decision and order of the Court.



2/11/2020
DATE

SALIANN SCARPULLA, J.S.C.

CHECK ONE:		CASE DISPOSED			X	NON-FINAL DISPOSITION	
		GRANTED	X	DENIED		GRANTED IN PART	OTHER
APPLICATION:		SETTLE ORDER				SUBMIT ORDER	
CHECK IF APPROPRIATE:		INCLUDES TRANSFER/REASSIGN				FIDUCIARY APPOINTMENT	REFERENCE