

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

MARK SKAPINETZ

Plaintiff,

v.

COESTERVMS.COM, INC.
et al.,

Defendants.

*

*

*

*

*

*

Civil Action No. PX-17-1098

MEMORANDUM OPINION

Pending before the Court is a Motion to Dismiss under Federal Rule of Civil Procedure 12(b)(6) filed by Defendants COESTERVMS.COM INC. and Brian Coester. The Court has reviewed the parties' submissions and rules pursuant to Local Rule 105.6 because no hearing is necessary. For the reasons stated below, the Defendants' motion is granted in part and denied in part.

I. BACKGROUND

Mark Skapinetz is a real estate appraiser in Atlanta, Georgia. At all times relevant to this lawsuit, Skapinetz maintained two email accounts related to his real estate appraisal business, What's it Worth Appraisal Services, LLC. One account, the *wiwapp@gmail.com* ("wiwapp account"), was exclusively dedicated to Skapinetz's business. ECF No. 1 at ¶¶ 16–17. The second account, *mappraiser14@gmail.com*, was used "for his more personal dealings related to real estate and real estate appraisals." *Id.* at ¶18. The *mappraiser14* account was not publicly linked to Skapinetz and he did not maintain many emails in the account. *Id.* at ¶¶ 49 & 50.

Skapinetz's email host, Google or Gmail, allows users to personalize their "security options" to receive notifications if someone signs onto the account from a new location or

device. Skapinetz opted to use this security feature and supplied his business telephone number, (404) 421-0055 (“0055 number”), as the contact for notifications for both the wiwapp and mappraiser14 accounts. *Id.* at ¶ 19. The 0055 number is publicly available and an internet search for it will produce results about Skapinetz and his appraisal company. *Id.* at ¶ 20–21.

From April 2014 through April 2016, Skapinetz performed real estate appraisals as a subcontractor for Defendant CoesterVMS.com Inc. located in Rockville, Maryland. *Id.* at ¶¶ 6,7, 10, 22. Defendant Brian Coester, a resident of the state of Maryland, is the owner, principal, and resident agent of CoesterVMS.com Inc. *Id.* at ¶¶ 8–13. Shortly after terminating his business relationship with the Defendants, Skapinetz learned of a fraud lawsuit that CoesterVMS’ former employees had filed against Defendants. *Id.* at ¶¶ 24–25. Skapinetz then composed and sent an “anonymous” email on November 11, 2016 from the mappraiser14account to a number of his colleagues which discussed Defendants’ lawsuit and their general business practices. *Id.* at ¶ 26.

At or around 11:09 a.m. the same day, Skapinetz received an email at the mappraiser14 account from bcoester@coesterappraisals.com (“bcoester account”), which Skapinetz alleges is an e-mail address used by Defendant because the domain name “coesterappraisal.com” is owned by Brian Coester and Coester Appraisal Services. *Id.* ¶ 35–36. The email stated that the sender “will be in touch soon, I understand that you have an issue with myself and have decided to e-mail our clients about this and inappropriately mischaracterizing [sic] the nature of the suit and also the faculty [sic] allegations” in the Defendants’ pending lawsuit. *Id.* at ¶ 42. This email did not address Skapinetz by name. *Id.*

Shortly after, at about 11:19 a.m., Gmail sent Skapinetz a security alert which notified him that a device in Maryland using “Chrome from Windows” had signed into the mappraiser14 account. ECF No. 1 at ¶27–28. Skapinetz became concerned because neither he nor any of his

devices were presently located in Maryland. *Id.* at ¶ 15. Between 11:19 a.m. and 12:51 p.m., a device using the same IP address of 2601:152:4202:5f00:35bb:3cd6:f465:b31d repeatedly accessed Skapinetz’s mappraiser14 and wiwapp accounts. *Id.* at ¶ 29. Around 12:22 p.m., Skapinetz received a second email from the bcoester account, stating “Mark – we have been able to verify this is you . . . Brian.” *Id.* at ¶ 44.

On January 7, 2017, Skapinetz received a message from Defendants via the social media platform Twitter regarding the anonymous email. ECF No. 1 at ¶ 71; *see also* ECF Nos. 1-7 & 1-8. Skapinetz then accused Defendants of hacking into his email account, to which Defendant Brian Coester replied that he did not “have a clue what you’re talking about other then [sic] you sent an email to Dave, Dave sent it to me and I sent it to my IT who said it was you.” ECF No. 1 at ¶ 75.

On April 20, 2017, Skapinetz filed this action for injunctive relief and damages, alleging violations of the Stored Communications Act (“SCA”), 18 U.S.C. §§ 2701(a) & 2707, and asserting common law claims for trespass to chattels, trespass to land, conversion, fraud and invasion of privacy. Skapinetz essentially avers that Defendants hacked into Skapinetz’ mappraiser14 email account, which allowed Defendants to learn he was the sender of the anonymous email. *Id.* at ¶56–59. Defendants filed a motion to dismiss on May 24, 2017, arguing that Skapinetz’s Complaint fails to state claims for relief under the SCA and that the court should decline to exercise supplemental jurisdiction over the remaining claims. ECF Nos. 9 & 10. Defendants also raise a number of substantive challenges to Plaintiff’s common law claims. *Id.*

II. STANDARD OF REVIEW

When reviewing a motion to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6), a court must determine whether the complaint includes facts sufficient to state a claim to relief that is plausible on its face. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). Factual allegations in the complaint are taken as true, but a court need not credit legal conclusions couched as fact. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). A plaintiff must plead facts to support each element of the claim to satisfy the standard. *See McCleary-Evans v. Maryland Dept. of Transp., State Highway Admin.*, 780 F.3d 582, 585 (4th Cir. 2015).

Further, when a plaintiff alleges fraud, Rule 9(b) of the Federal Rules of Civil Procedure requires that such claims be pleaded with particularity. *Haley v. Corcoran*, 659 F. Supp. 2d 714, 721 (D. Md. 2009) (quoting *Adams v. NVR Homes, Inc.*, 193 F.R.D. 243, 250 (D. Md. 2000); Fed. R. Civ. P. 9(b)). To satisfy this standard, a plaintiff “must, at a minimum, describe the time, place, and contents of the false representations, as well as the identity of the person making the misrepresentation and what he obtained thereby.” *United States ex rel. Wilson v. Kellogg Brown & Root, Inc.*, 525 F.3d 370, 379 (4th Cir. 2008) (internal quotation marks and citation omitted). “These facts are often referred to as the ‘who, what, when, where, and how’ of the alleged fraud.” *Id.* (quoting *United States ex rel. Willard v. Humana Health Plan of Tex. Inc.*, 336 F.3d 375, 384 (5th Cir. 2003)). This requirement affords the defendants notice of the basis for the claim, safeguards against frivolous suits, and minimizes the risk of unwarranted damage to the defendant’s reputation. *Harrison v. Westinghouse Savannah River Co.*, 176 F.3d 776, 783 (4th Cir. 1999) (citation omitted). Fraud allegations that fail to comply with Rule 9(b) must be dismissed pursuant to Rule 12(b)(6). *Id.* at 783 n.5.

III. ANALYSIS

a. Stored Communications Act

Skapinetz argues that Defendants are subject to civil liability under the SCA for allegedly accessing his email accounts without authorization. *See* 18 U.S.C. § 2707(a) (providing for a private, civil cause of action for knowing or intentional violations of the SCA). To sustain a claim under the SCA, a plaintiff must demonstrate that a person intentionally accessed “without authorization a facility through which an electronic communication service is provided” and “thereby obtain[ed], alter[ed], or prevent[ed] authorized access to a wire or electronic communication while it is in electronic storage in such system[.]” *Id.* § 2701(a). Defendants argue that Skapinetz has failed to plead facts sufficient to aver plausibly that Defendants: (1) accessed Skapinetz’s emails while they were in “electronic storage;” as defined by the SCA; (2) *intentionally* accessed Skapinetz’s email accounts; and (3) obtained, altered, or prevented authorized access to Skapinetz’s emails. *See* ECF No. 10 at 4–16. The Court addresses each contention in turn.

The SCA defines “electronic storage” as “(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication[.]” 18 U.S.C.A. § 2510(17); *see also id.* § 2711(1) (incorporating the definitions in § 2510 for purposes of the SCA). Defendants argue that Skapinetz has not sufficiently pled that the emails were in “electronic storage” because he does not allege particular facts as to the nature and status of the particular emails “obtained” by Defendants. *See* ECF No. 10 at 15. In response, Skapinetz argues that the SCA merely requires unauthorized access to email communications stored on a cloud-based e-mail account, as was the

case here. ECF Nos. 1 at ¶¶ 117, 119 & 14 at 8–11; see *Theofel v. Farey-Jones*, 359 F.3d 1066, 1077 (9th Cir. 2004) (finding that within the ordinary meaning of § 2510(17)(B)’s terms, emails on the server of an internet service provider for purposes of backup protection are in “electronic storage” as defined by § 2510(17)(B)). Skapinetz also points to a number of courts which have found that a properly stated claim under the SCA does not turn on “whether an email stored on an internet service provider’s server has been opened or not.” *Hoofnagle v. Smyth-Wythe Airport Commission*, Case No. 15-8, 2016 WL 3014702 at *10 (W.D. Va. May 24, 2016); see also *Pure Power Boot Camp, Inc., et al v. Warrior Fitness Boot Camp, et al*, 587 F. Supp. 2d 548, 555–56 (S.D.N.Y. 2008); accord *Levin v. ImpactOffice LLC*, Case No. TDC-16-2790, 2017 WL 2937938 at *3 (D. Md. Jul 10, 2017) (rejecting plaintiff’s argument that “temporary, intermediate storage” includes “all stored electronic communications” but finding that she was not required to “specifically state in the complaint” the status of the emails allegedly accessed by defendant). Based on the plain language of the SCA and courts’ interpretation of “electronic storage,” Defendants’ argument must fail. Plaintiff sufficiently pled that the emails were in the “electronic storage” of their internet service provider, Google, at the time of Defendants’ unauthorized access. These allegations survive a motion to dismiss.

Defendants next argue that Plaintiff has not pled that Defendants accessed Skapinetz’s email accounts with a “knowing or intentional state of mind.” See ECF No. 10 at 13–15. “ ‘Intentional’ means more than that one voluntarily engaged in conduct or caused a result. Such conduct or the causing of the result must have been the person’s conscious objective.” *Butera & Andrews v. IBM Corp., et al.*, 456 F. Supp. 2d 104, 109 (D.D.C. 2006) (quoting the United States Senate Committee on the Judiciary report on the Electronic Communications and Privacy Act of 1986, S. Rep. No 99–541, at 23 (1986)). Skapinetz has pleaded just that. Skapinetz repeatedly

alleges that Defendants took purposeful steps to obtain access to and review the contents of Skapinetz's protected email accounts. *See, e.g.*, ECF No. 1 at ¶¶ 48, 51, 53, 55, 56, 63, 64–66, 118. Skapinetz has undoubtedly averred that Defendants, by purposefully accessing his email accounts with the express intent of observing their communications, possessed a “knowing or intentional state of mind.”

As to Defendants' third contention, Defendants argue that Skapinetz must state with particularity that they “obtained” specific emails during their unauthorized access of Skapinetz's email account to sustain an SCA claim. ECF No. 10 at 9–10. Defendants note that “in virtually [sic] all cases where a civil action under the SCA was upheld, . . . some *use* of those communications was proven – e.g., they were downloaded, printed, or otherwise utilized in some affirmative manner.” *Id.* at 11–12. None of these cases, however, stand for the proposition that where the plaintiff alleges that defendant accessed emails and made use of their content, the defendant has not “obtained” the email as a matter of law. *Cf. Pure Power Boot Camp, Inc., et al v. Warrior Fitness Boot Camp, Inc., et al*, 759 F. Supp. 2d 417 (S.D.N.Y. 2010) (granting summary judgment on a third-party complaint where discovery revealed that plaintiffs repeatedly accessed defendants' email accounts and attempted to use defendants' printed emails as evidence in their lawsuit); *Global Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 631 (E.D. Va. 2009) (denying a motion to dismiss where the defendant admitted to accessing plaintiff's email accounts but argued his access was authorized); *Hoofnagle v. Smyth-Wythe Airport Commission*, Case No. 15-8, 2016 WL 3014702 (W.D. Va. May 24, 2016); (denying summary judgment where the defendants admitted accessing the plaintiff's email account but a material question of fact remained as to authorization).

Nor would such a ruling comport with the plain meaning of “obtain.” Black’s Law Dictionary defines obtain as “to bring into one’s possession; to procure, especially through effort.” *Obtain*, Black’s Law Dictionary (10th ed. 2014). Similarly, Merriam Webster’s Dictionary defines obtain as “to gain or attain, usually by planned action or effort,” noting by way of illustration, “[t]he information was difficult to obtain.” *Obtain*, Merriam-Webster.com, <https://www.merriam-webster.com/dictionary/obtain> (last visited Feb. 7, 2018). Nowhere does the term “obtain” require more than coming into possession of *information*, which is what Skapinetz has pleaded here. Skapinetz particularly asserts that Defendants gained unauthorized access to his emails, and then contemporaneously informed Skapinetz that Defendants knew of his sending an otherwise anonymous email message about Defendants’ lawsuit and company. A reasonable and plausible inference, therefore, is that Defendants “obtained” the information that Skapinetz authored the anonymous email by accessing Skapinetz’s email accounts without permission. Skapinetz also specifically alleges that Defendants reviewed all of his emails in both accounts. *See* ECF No. 1 at ¶¶ 55 & 56. Defendants’ argument is thus unavailing.

Finally, Defendants vaguely assert that the SCA claim must be dismissed because the SCA targets “computer hackers (e.g. electronic trespassers)” and “Defendants are certainly not ‘hackers’ as that term is understood by anyone.” ECF No. 10 at 7 (quoting *Int’l Assoc’n of Machinists & Aerospace Workers v. Werner-Masuda, et al.*, 390 F. Supp. 2d 479, 495–96 (D. Md. 2005)). The Court disagrees. The Complaint alleges facts that, if true, constitute an electronic trespass or computer hacking as the term is commonly used. Accordingly, the Motion to Dismiss the SCA claim (Count One) is DENIED.

b. State Law Claims

Skapinetz brings state common law claims for trespass to land, chattels, conversion, fraud, and invasion of privacy – intrusion upon seclusion. ECF No. 1. Defendants argue that dismissal is warranted because Maryland law does not apply to Plaintiff’s tort claims or, in the alternative, that the claims are not adequately pled under Maryland common law. The Court, exercising supplemental jurisdiction over these claims, applies Maryland’s choice of law rules. *See Klaxon Co. v. Stentor Elec. Mfg. Co.*, 313 U.S. 487, 496 (1941); *ITCO Corp. v. Michelin Tire Corp., Commercial Div.*, 722 F.2d 42, 49 n.11 (4th Cir. 1983), *cert denied*, 469 U.S. 1215 (1985). Maryland applies the state’s substantive law for tort claims based on the *lex loci delicti commissi*, or place of harm rule. *Hauch v. Connor*, 295 Md. 120, 123–24, 453 A.2d 1207 (1983). “[W]here the events giving rise to a tort action occur in more than one State, we apply the law of the State where the injury – the last event required to constitute the tort – occurred.” *Lab. Corp. of Am. v. Hood*, 395 Md. 608, 615, 911 A.2d 841 (2006) (citing cases).

i. Trespass to Chattels and Conversion

Skapinetz pleads that Defendants committed the torts of trespass and conversion by accessing without authorization, and intermeddling with, Skapinetz’s email accounts and electronic communications. ECF No. 1 at ¶¶ 125–29; 141. Although email accounts and electronic communications are not tangible property in the traditional sense, many courts have recognized claims for conversion or trespass to chattels involving digital “property.” *See, e.g., Ground Zero Museum Workshop, et al. v. William Wilson*, 813 F. Supp. 2d 678, 697 (D. Md. 2011); *Astroworks, Inc. v. Astroexhibit, Inc.*, 257 F. Supp. 2d 609, 618 (S.D.N.Y. 2003); *Am. Online, Inc. v. IMS*, 24 F. Supp. 2d 548, 550 (E.D. Va. 1998). For torts of conversion and intermeddling with chattels, the injury occurs either at “the place where [the plaintiff was]

located at the time of the alleged trespass, or the law of the place where the chattel was located.”
Ground Zero, 813 F. Supp. 2d at 697.

At the time Defendants allegedly accessed Skapinetz’ email accounts, Skapinetz was physically in Georgia, and the property – the emails – were in the possession of the email provider, Google. ECF No. 1 at ¶ 15. Neither party addresses the precise location of Skapinetz’s emails. However, the Court notes that Google stores email communications on servers located throughout the United States and abroad. *See, e.g. Porters Building Centers, Inc. v. Sprint Lumber*, No. ODS-16-6055, 2017 WL 4413288 at *11 (W.D. Mo. Oct. 2, 2017); *In re Search Warrant No. 16-960-M-1 to Google*, No. 16-960, 2017 WL 3535037, at *1 (E.D. Pa. Aug. 17, 2017); *In re Search of Info. Associated with [redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc.*, No. 16-757, 2017 WL 3445634, at *2 (D.D.C. July 31, 2017); *In re Search Warrant to Google, Inc.*, No. 16-4116, 2017 WL 2985391, at *2 (D. N.J. July 10, 2017). Electronic communications stored by Google “are on a dynamic network” that frequently and automatically moves data from one location to another, such that different components of a single email may be stored on multiple servers. *See, e.g., In re Search of Info. Associated with [redacted]@gmail.com*, 2017 WL 3445634 at *2; *In re Search Warrant to Google, Inc.*, 2017 WL 2985381 at *2; *Matter of Search of Information Associated with [redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc.*, No. GMH-16-757, 2017 WL 2480752 at *3 (D.D.C. June 2, 2017).

Based on the above, the Court takes judicial notice regarding the manner in which “Gmail” electronic communications are stored on servers. Accordingly, the question of the applicable state common law is less than straightforward. At this stage, the Court cannot practically apply the law where the property is located, as that is unknown and potentially

involves multiple Google servers at the time of the trespass. The Court will therefore apply Georgia law, where Skapinetz was located when his personal property interest was harmed by Defendants' trespass.

Georgia defines trespass to chattel as “[a]ny unlawful abuse of or damage done to the personal property of another.” O.G.C.A. § 51-10-3. In *AT&T Mobility LLC v. Does 1–4*, No. JOF-09-277, 2011 WL 13213864 (May 26, 2011), the United States District Court for the District of Georgia considered “the issue of trespass in the context of computer and telephone systems” and found that the defendants, by sending “millions of unauthorized telemarketing calls,” interfered with Plaintiff’s property rights. *AT&T Mobility LLC*, 2011 WL 13213864 at *2. Here, unlike *AT&T Mobility LLC*, Skapinetz does not allege that Defendants’ trespass “actually burdened” his property rights or damaged the “chattels.” See ECF No. ¶127–28. However, Georgia courts have not affirmatively required that actual damages are needed to sustain a claim of electronic trespass, and favorably cite to courts holding otherwise. See, e.g. *Etzel v. Hooters of America, LLC*, 223 F. Supp. 3d 1306, 1314 (N.D. Ga. 2016) (citing *Mey v. Got Warranty, Inc.*, 193 F. Supp. 3d 641, 647 (N.D. W. Va. 2016) for the proposition that “the mere invasion of the consumer’s electronic device can be considered a trespass to chattels.”). Further, if the mere act of sending unwanted emails into a person’s email account can constitute trespass to chattels, it logically follows that a person’s *direct* unauthorized access on another’s email accounts would also present an actionable claim. See, e.g. *America Online, Inc. v. IMS*, 24 F. Supp. 2d 548, 550 (E.D. Va. 1998); see also Richard Warner, *Border Disputes: Trespass to Chattels on the Internet*, 47 Vill. L. Rev 117 (2002). Accordingly, Skapinetz has stated a plausible claim for trespass to chattels, and Defendants’ Motion to Dismiss Count Two is DENIED.

As to conversion under Georgia law, “tangible personalty or specific intangible property may be subject for an action for conversion.” *See Taylor v. Powertel, Inc.*, 250 Ga. App. 356, 358-59 (2001). Conversion is defined as “the unauthorized assumption and exercise of the right of ownership over personal property belonging to another which is contrary to the owner's rights.” *Taylor v. Gelfand*, 233 Ga. App. 835, 837 (1998) (quoting *Reeves v. Edge*, 225 Ga. App. 615, 619 (1997)). “Any act of dominion wrongfully asserted over another's personal property which is in denial of his property rights, or inconsistent with them, is a conversion.” *Ewaldsen v. Atlantic Ins. Brokers, L.L.C.*, 267 Ga. App. 347, 349 (2004) (citations and quotation marks omitted). To make out a prima facie case of conversion in Georgia, a plaintiff must show “title to the property, possession by the defendant, demand for possession, and refusal to surrender the property.” *Taylor*, 250 Ga. App. at 358. However, when a plaintiff contends that a defendant came into possession of the property unlawfully, the plaintiff need not show a demand for the property and a refusal to return it to establish their claim. *See AT&T Mobility LLC v. Does 1–4*, Case No. JOF-09-277, 2012 WL 13001387 at *3 (N.D. Ga. Mar. 29, 2012) (denying a motion to dismiss where plaintiff pled that telemarketers exercised wrongful dominion and control over their property by sending unauthorized telemarketing calls).

The Complaint alleges that Defendants committed conversion through their assertion of “ownership and dominion over Skapinetz’s Gmail accounts and e-mail communications” that gave Defendants the “same access to Plaintiff’s e-mail communications as an authorized user would have, inconsistent with Plaintiff’s right to exclusive ownership.” ECF No. 1 at ¶ 141. These facts, taken as true, plausibly establish that Defendants assumed and exercised the right of ownership over Skapinetz’s email accounts, albeit briefly, and these actions were inconsistent

with Skapinetz's property rights. *See* ECF No. 1 at ¶¶ 27–69. Therefore, Defendant's Motion to Dismiss the common law claim for conversion (Count Four) is DENIED.

ii. Trespass to Land

When trespass to land is alleged, Maryland's "place of harm" principle requires courts to look to where the "land is situated." *Accord Piven v. Comcast Corp.*, 397 Md. 278, 284 (Court of Appeals of Maryland 2007) (discussing Maryland's requirement that the claim is brought in the county where the harm occurred); *MCI Communications Services, Inc. v. American Infrastructure-MD, Inc.*, GLR-11-3767, 2013 WL 4086401, at *15 (D. Md. Aug. 12, 2013). However, as Defendants note in their Motion to Dismiss, the Complaint does not allege a trespass to land *at all*, so it is impossible to establish where the "land" is situated. *See* ECF No. 10 at 20–21. The Court cannot meaningfully analyze the "choice of law" for Skapinetz's claim, or otherwise evaluate its sufficiency. Further, no reasonable person could construe Skapinetz's admittedly intangible property interest in his email accounts as land. Defendants' Motion to Dismiss Skapinetz's common law claim for trespass to land (Count Three) is GRANTED.

iii. Fraud

Skapinetz's claim of fraud is based on Defendants' "misrepresentations" in a series of electronic communications that they "were not responsible for the unauthorized accesses of Plaintiff's Gmail accounts," which then caused Plaintiff to delete his mappraser14 email account, "losing business records, confidential data, and client and colleague contact information." ECF No. 1 at ¶¶ 70, 75–76, 145–49; *see also* ECF Nos. 1-5 & 1-7. Claims for fraud are also governed by the law of the place of injury, but the Complaint does not state where the acts giving rise to the claim occurred. *See* ECF No. 1 at ¶¶ 145–50. The Court, therefore, will GRANT

Defendants' Motion to Dismiss without prejudice and with leave for Skapinetz to amend his fraud count (Count Five) within fourteen (14) days to clarify the situs of injury.

iv. Invasion of Privacy – Intrusion on Seclusion

For Skapinetz's invasion of privacy claim, Maryland again requires that the Court apply the substantive law of the state of the "place of harm." The harm asserted in Skapinetz's "invasion of privacy – intrusion upon seclusion" is Defendant's alleged viewing in Maryland of the protected contents of Skapinetz's email account, resulting in injury to Skapinetz in Georgia. *See* ECF No. 1. Both Maryland and Georgia apply the Restatement (Second) of Torts which provides that intrusion on seclusion is actionable when (1) defendant intruded or pried into a person's private concerns; and (2) a reasonable person would find the intrusion offensive or objectionable. Restatement (Second) of Torts § 652B (1977); *Mitchell v. Balt. Sun. Co.*, 164 Md. App. 497, 522 (2005); *Yarbray v. Southern Bell Tel. & Tel. Co.*, 261 Ga. 703, 705 (1991).

Intrusion on seclusion often "involves physical intrusion into a place where a plaintiff has secluded [him]self," but "may also occur 'by some other form of investigation or examination into [the plaintiff's] private concerns.'" *Noshafagh v. Leggett*, No. DKC-11-3038, 2013 WL 93345 at *15 (D. Md. Jan. 7, 2013) (quoting Restatement (Second) of Torts § 652B cmt. b)); *see also Anderson v. Mergenhagen*, 283 Ga. App. 546, 55–510 (2007) (noting that Georgia courts have extended principle beyond physical intrusion to "prying and intrusions into private concerns."). Opening or examining a person's private correspondence without consent is an examination into private concerns and is thus actionable. *See* Restatement (Second) of Torts § 652B cmts. b, c. Therefore, taking the facts alleged in the Complaint as true, Defendants' hacking of Skapinetz's email accounts and review of his emails is an intrusion into his private concerns.

As to whether a reasonable person would find this intrusion “offensive or objectionable,” Defendants’ sole argument is that the Complaint “alleged nothing that remotely satisfies” the “reasonable person” standard. *See* ECF No. 10 at 22–23. The Court disagrees. Skapinetz avers that Defendants accessed his password protected email accounts and reviewed the email content for several hours. ECF No. 1 at ¶¶ 29, 46, 52–56, 63–67. A reasonable person could certainly find such an intrusion “offensive or objectionable.” *See Coughlin v. Town of Arlington*, No. MLW-10-10203, 2011 WL 6370932, at *10 (D. Ma. Dec. 19, 2011); *Peterson v. Aaron’s, Inc.*, No. TWT-14-1919, 2017 WL 4390260, at *4–*7 (N.D. Ga. Oct. 3, 2017); *see also Murphy v. Spring*, 58 F. Supp. 3d 1241, 1271 (N.D. Ok. 2014); *Mintz v. Mark Bartelstein and Associates Inc.*, 906 F. Supp. 2d 1017, 1033–34 (C.D. Ca. 2012); *Brown-Criscuolo v. Wolfe*, 601 F. Supp. 2d 441, 449–50 (D. Ct. 2009); *Doe v. City and County of San Francisco*, No. TEH-10-4700, 2012 WL 2132398, at *4–*5 (N.D. Ca. June 12, 2012); *Thayer Corp. v. Reed*, No. JAW-10-423, 2011 WL 2682723, at *10 (D. Me. July 11, 2011). Nor does the analysis differ under Georgia or Maryland law. The parties are free, however, to address the choice of law question in any dispositive motions filed at the close of discovery, if necessary.

IV. CONCLUSION

For the foregoing reasons, Defendants’ Motion to Dismiss is DENIED as to all claims except Counts Three and Five, which are DISMISSED. Plaintiff has fourteen (14) days from the issuance of this Opinion to amend Count Five. A separate Order follows.

2/9/2018

Date

/S/

Paula Xinis

United States District Judge