

Source: Legal > / ... / > VA Federal District Courts 

Terms: name(global policy partners and yessin) (Edit Search | Suggest Terms for My Search)

2009 U.S. Dist. LEXIS 112472, *

GLOBAL POLICY PARTNERS, LLC, et al., Plaintiffs, v. BRENT YESSIN, Defendant.

No. 1:09cv859

UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA, ALEXANDRIA DIVISION

2009 U.S. Dist. LEXIS 112472

November 24, 2009, Decided

CASE SUMMARY


PROCEDURAL POSTURE: Plaintiffs, a wife and a company, alleged that defendant husband was liable under the Computer Fraud and Abuse Act, 18 U.S.C.S. § 1030(a), the Electronic Communications Privacy Act, 18 U.S.C.S. § 2511, the Stored Communications Act, 18 U.S.C.S. § 2701, and Va. Code §§ 19.2-62 (A), 18.2-152.3, 18.2-152.5, which criminalize unauthorized access to, or interception of, communications. The husband sought to dismiss or to stay.

OVERVIEW: The parties were feuding business partners who were - not incidentally - also feuding marriage partners in the process of dissolving their marriage, as well as their business relationship. Allegedly, the husband accessed and intercepted his wife's business e-mail, without authorization, in order to review messages between the wife and her attorney related to the pending contested divorce proceeding. The court held that because the wife and company did not allege facts creating a plausible inference that the husband intercepted any communications, nor had they forecasted any factual allegations that would create such a plausible inference, these claims failed to survive dismissal. Moreover, the wife and company neither alleged nor forecasted facts that would sustain a conclusion that the husband examined certain sensitive information or obtained, embezzled, or converted any property. However, the wife and company did plead sufficient facts to create a plausible inference that the husband lacked authorization to access the wife's e-mail account. Finally, whether the company was validly a party to this suit was not an issue that could properly be decided solely on the pleadings.

OUTCOME: The husband's motion to dismiss was granted in part, and only denied as to four counts where the wife and company pleaded sufficient facts to create a plausible inference that the husband lacked authorization to access the wife's e-mail account. There is not good cause to stay this proceeding pending the outcome of the declaratory judgment suit action brought by Mr. Yessin in a Florida court.


CORE TERMS: e-mail, intercept, manager, network, authorization, message, server, stored, factual allegations, intercepted, accessing, unauthorized, interception, password, electronic communications, appropriately, transmission, electronic, divorce proceeding, destination, threshold, accessed, oral communication, conversion of property, intentionally, declaratory, embezzled, converted, endeavor, wire

[Civil Procedure](#) > [Pleading & Practice](#) > [Defenses, Demurrers & Objections](#) > [Failures to State Claims](#) 


HN1  [Threshold dismissal pursuant to Fed. R. Civ. P. 12\(b\)\(6\) must be granted unless the complaint contains sufficient factual matter, accepted as true; to state a claim to relief that is plausible on its face. It follows that to survive a Rule 12\(b\)\(6\) motion to dismiss, a complaint must contain more than an unadorned, the-defendant-unlawfully-harmed-me accusation. And in this respect, it is also true that the tenet that a court must accept as true all of the allegations contained in a complaint is inapplicable to legal conclusions. Thus, threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice.](#) [More Like This Headnote](#)

[Computer & Internet Law](#) > [Privacy & Security](#) > [Company Communications](#) 


[Computer & Internet Law](#) > [Privacy & Security](#) > [Invasion of Privacy](#) 


HN2  Courts have generally and sensibly concluded that the scope of an individual's authorization to access a computer network is analyzed on the basis of the expected norms of intended use. In other words, authorization to access a computer network may not, in some cases, turn simply on a person's status or position in a company because the expected norms of intended use of the network may indicate otherwise. Accordingly, whether authorization exists may require a factual inquiry beyond the scope of the threshold motion stage. [More Like This Headnote](#)

[Business & Corporate Law](#) > [Limited Liability Companies](#) > [Management Duties & Liabilities](#) 


HN3  [Fla. Stat. § 608.4235](#), which, in the course of entitling managers to act as agents of an limited liability company (LLC) for the purpose of carrying out the LLC's ordinary business, specifies that managers of LLC may sign and deliver any instrument transferring or affecting the limited liability company's interest in real property. [Fla. Stat. § 608.4235.](#) [More Like This Headnote](#)

[Computer & Internet Law](#) > [Privacy & Security](#) > [Electronic Communications Privacy Act](#) 


HN4  The Electronic Communications Privacy Act (ECPA), in part, prohibits intentionally intercepting any electronic communication. [18 U.S.C.S. § 2511\(1\)\(a\)](#). The act further defines "intercept" to mean the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device. [18 U.S.C.S. § 2510\(4\)](#). A Virginia statute, [Va. Code § 19.2-62\(A\)](#), essentially parrots the federal statute. Indeed, the Supreme Court of Virginia has forthrightly stated that [Va. Code § 19.2-62](#) is Virginia's version of the ECPA. And the Virginia Code defines "intercept" in terms virtually identical to the ECPA's definition. [Va. Code § 19.2-61](#). Thus, the term "intercept" in [Va. Code § 19.2-62](#) is appropriately construed and applied in precisely the same way as its federal counterpart. [More Like This Headnote](#)

[Communications Law](#) > [Privacy](#) > [Stored Communications Act](#) 


[Computer & Internet Law](#) > [Privacy & Security](#) > [Electronic Communications Privacy Act](#) 

HN5  Courts applying the Electronic Communications Privacy Act (ECPA) have consistently held that a qualifying "intercept" occurs only where the acquisition of the communication occurs contemporaneously with its transmission by its sender. Thus, interception includes accessing messages in transient storage on a server during the course of transmission, but does not include accessing the messages stored on a destination server. A qualifying "intercept" under the ECPA and [Va. Code § 19.2-62](#) can only occur where an e-mail communication is accessed at some point between the time the communication is sent and the time it is received by the destination server, at which point it becomes a "stored communication" within the meaning of the Stored Communications Act. Thus, accessing a stored communication does not constitute an "intercept" within the meaning of the ECPA or [Va. Code § 19.2-62](#). [More Like This Headnote](#)




[Computer & Internet Law](#) > [Criminal Offenses](#) > [Data Crimes & Fraud](#) 

HN6  [Va. Code § 18.2-152.3](#), creates a civil remedy against any person who uses a computer or computer network, without authority and: (i) obtains property or services by false pretense, (ii) embezzles or commits larceny, or (iii) converts the property of another. [More Like This Headnote](#)

[Computer & Internet Law](#) > [Criminal Offenses](#) > [Data Crimes & Fraud](#) 

HN7  [Va. Code § 18.2-152.5](#), prohibits unauthorized use of a computer network to examine employment, salary, credit, or other financial or identifying information. To state a valid claim under this statute, plaintiffs must allege facts creating a plausible inference that a defendant (i)

uses a computer or computer network (ii) without authority, (iii) with the intent to examine another's records, (iv) without authority, and (v) the records contained employment, salary, credit, or other financial or identifying information as defined by the statute. Plaintiffs must allege facts that, if true, create plausible inferences that these elements are satisfied. [More Like This Headnote](#)

COUNSEL: **[*1]** For Global Policy Partners, LLC, Katherine Friess Yessin, Plaintiffs: [Bernard Joseph DiMuro](#) , [Stephen James Stine](#) , LEAD ATTORNEYS, DiMuro Ginsberg & Mook PC, Alexandria, VA; [Stacey Rose Harris](#) , LEAD ATTORNEY, DiMuro Ginsberg PC, Alexandria, VA.

For Brent Yessin, Defendant: [Charles Michael Sims](#) , LEAD ATTORNEY, LeClairRyan, A Professional Corporation, Richmond, VA; [C. Matthew Haynes](#) , LeClair Ryan PC (Alexandria), Alexandria, VA.

JUDGES: [T. S. Ellis, III](#) , United States District Judge.

OPINION BY: [T. S. Ellis, III](#) 

OPINION

MEMORANDUM OPINION

This is a dispute between feuding business partners who are--not incidentally--also feuding marriage partners in the process of dissolving their marriage, as well as their business relationship. According to the complaint, the husband accessed and intercepted his wife's business e-mail, without authorization, in order to review messages between the wife and her attorney related to the pending contested divorce proceeding. Accordingly, plaintiffs allege that defendant is liable under (i) the Computer Fraud and Abuse Act (CFAA), [18 U.S.C. § 1030\(a\)](#), (ii) the Electronic Communications Privacy Act (ECPA), [18 U.S.C. § 2511](#), (iii) the Stored Communications Act (SCA), [18 U.S.C. § 2701](#), and **[*2]** (iv) three Virginia statutes ([Va. Code § 19.2-62 \(A\)](#), [Va. Code § 18.2-152.3](#), and [Va. Code § 18.2-152.5](#)) criminalizing unauthorized access to, or interception of, communications. Defendant seeks threshold dismissal of these claims pursuant to [Rule 12 \(b\)\(6\), Fed. R. Civ. P.](#), on the grounds that (i) any access to the communications was authorized, and (ii) he did not intercept the communications within the meaning of the relevant statutes. Alternatively, he requests a stay of this case pending the outcome of a declaratory judgment proceeding currently pending in a Florida court.

The matter was fully briefed, and oral argument was heard on October 9, 2009, following which a ruling issued from the bench, which ruling was subsequently memorialized by Order. This Memorandum Opinion elucidates the reasons for the ruling on defendant's motion.

I. ¹

FOOTNOTES

¹ The facts recited herein are derived largely from plaintiffs' complaint and are, as required at this stage in the proceedings, assumed to be true. *See Revene v. Charles County Comm'rs*, 882 F.2d 870, 872 (4th Cir. 1989); *see also Ashcroft v. Iqbal*, 129 S. Ct. 1937, 1950, 173 L. Ed. 2d 868 (2009) ("When there are well-pleaded factual allegations, a court should assume **[*3]** their veracity and then determine whether they plausibly give rise to an entitlement to relief.").

The individual plaintiff, Katherine Yessin, is a lawyer and a citizen of Virginia. She is currently married to defendant Brent Yessin, a citizen of Florida who is also a lawyer. Mrs. and Mrs. Yessin are in the midst of a contested divorce. The second plaintiff is Global Policy Partners, LLC ("GPP") a limited liability company established under the laws of the state of Florida and engaged in the business of lobbying and business consulting. Plaintiffs allege that Mr. and Mrs. Yessin were two of three managers of GPP within the meaning

of Florida law. ² The third manager, Jeffrey Weiss, is not a party to this action, but plaintiffs allege that he assented to bringing suit on GPP's behalf. It appears from the complaint that at the time of the alleged conduct, all three were managers of the company. Mr. Yessin now claims that he is the sole manager of GPP. In support of this claim, he submitted documents filed with the State of Florida purporting to remove Mrs. Yessin and Mr. Weiss as managers. Plaintiffs assert that these documents are fraudulent. ³ Plaintiffs further claim that GPP's policy **[*4]** during the relevant time involved "strictly protect[ing] and maintain [ing] the confidential and proprietary nature of its trade secrets, software," documents, communications, and services with passwords and other safeguards." Compl. P 10. Moreover, plaintiffs allege that Mr. Yessin did not have an account on the GPP computer server and thus lacked any authorization to access it.

FOOTNOTES

² See Fla. Stat. § 608.407 (setting out procedures for naming managers in the LLC's articles of incorporation).

³ It is neither appropriate nor necessary to resolve this disputed issue at this threshold stage; instead, plaintiffs' factual allegation that Mrs. Yessin and Mr. Weiss are managers of GPP must be assumed to be true.

According to the complaint, Mr. Yessin, on or about the date of their separation, May 24, 2009, began to log onto Mrs. Yessin's GPP e-mail account. The complaint does not address how this access was accomplished, but subsequent briefing suggests that he did so using the password that Mrs. Yessin had inadvertently stored on his computer. Plaintiffs allege that Mr. Yessin, in accessing Mrs. Yessin's GPP account, read her emails, which included some that she had not yet viewed. These messages **[*5]** included sensitive communications with her attorney concerning strategy in the divorce proceeding. Mrs. Yessin alleges she became suspicious that Mr. Yessin was accessing her e-mail account when he began using phrases during settlement negotiations that she and her divorce lawyer had used in their e-mail exchanges. Accordingly, Mrs. Yessin alleges she changed her password on June 25, 2009, and further alleges that Mr. Yessin then attempted, unsuccessfully, to obtain the new password from GPP's information technology specialist. Upon learning of these efforts, plaintiffs' counsel sent Mr. Yessin a letter demanding that he cease any efforts to access Mrs. Yessin's e-mail accounts. Plaintiffs allege that Mr. Yessin nonetheless continued to attempt to access Mrs. Yessin's e-mail account.

Thereafter, plaintiffs brought this suit against Mr. Yessin on July 31, 2009. They allege that through his conduct, Mr. Yessin has impaired the value of the GPP computer system and forced them to incur substantial costs in order to secure the network. Mrs. Yessin also alleges that she has suffered a loss of bargaining power in the ongoing divorce proceedings as a result of Mr. Yessin's conduct. Accordingly, **[*6]** plaintiffs seek relief under (i) the CFAA (Counts 1 and 2), (ii) the ECPA (Counts 3, 4, and 5), (iii) the SCA (Counts 6 and 7), (iv) Va. Code § 19.2-62(A) (Counts 8, 9, 10, and 11), (v) Va. Code § 18.2-152.3 (Count 12), and (vi) Va. Code § 18.2-152.5 (Count 13). Mr. Yessin filed his motion to dismiss on September 5, 2009, alleging that plaintiffs have failed to state valid claims upon which relief may be granted pursuant to Rule 12(b)(6), Fed. R. Civ. P. More specifically, Mr. Yessin argues (i) that he is a manager of GPP and as such he was authorized to access the computer network in question, (ii) that plaintiffs have not alleged facts sufficient to create a plausible inference that he "intercepted" communications within the meaning of governing federal and state laws, (iii) that they have not alleged any facts suggesting that Mr. Yessin obtained, embezzled, or converted property as required for one of the claims arising under Virginia law, (iv) that there are no factual allegations giving rise to plausible inferences that Mr. Yessin viewed employment or financial information as required under one of the Virginia law claims, and (v) that Mrs. Yessin lacks standing to bring suit on **[*7]** behalf of GPP. ⁴ Moreover, even assuming, *arguendo*, that valid claims have been stated, Mr. Yessin argues that this case should be stayed pending the outcome of a declaratory judgment action in Florida.

FOOTNOTES

⁴ In his original motion to dismiss, Mr. Yessin also argued (i) that plaintiffs failed to allege any damage or loss and (ii) that plaintiffs failed to state a valid trespass to chattels claim. Plaintiffs subsequently amended their complaint to include specific allegations of damages and to eliminate plaintiffs' trespass

to chattels claim. Accordingly, the portions of the motion to dismiss directed to the trespass to chattels claim and the absence of loss or damage allegations is appropriately denied as moot.

II.

The Supreme Court has recently and sensibly declared that ^{HN1} threshold dismissal pursuant to Rule 12(b) (6) must be granted unless the complaint "contain[s] sufficient factual matter, accepted as true; to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 129 S. Ct. 1937, 1949, 173 L. Ed. 2d 868 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570, 127 S. Ct. 1955, 167 L. Ed. 2d 929 (2007)). It follows that to survive a Rule 12(b)(6) motion to dismiss, a complaint must contain "more than an unadorned, [*8] the-defendant-unlawfully-harmed-me accusation." *Iqbal*, 129 S. Ct. at 1949. And in this respect, it is also true that "the tenet that a court must accept as true all of the allegations contained in a complaint is inapplicable to *legal* conclusions." *Id.* (emphasis added). Thus, "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Id.*, quoted in *Walker v. Prince George's County, Md.*, 575 F.3d 426, 2009 WL 2343614, at *5 (4th Cir. 2009) (O'Connor, J.). Accordingly, Mr. Yessin's motion to dismiss must be granted if the complaint does not allege a sufficient factual basis to create a plausible inference that plaintiffs are entitled to relief.

III.

A. Claims Alleging Unauthorized Access to Communications

Counts 1, 2, 6, 7, and 12 of the complaint allege civil liability on the ground that Mr. Yessin acted without authority or exceeded his authority in accessing or using a computer or computer network in violation of the CFAA, 18 U.S.C. § 1030(a), the SCA, 18 U.S.C. § 2701(a), Va. Code § 18.2-152.3, and Va. Code § 18.2-152.5. The CFAA prohibits, in pertinent part, "knowingly access[ing] a computer without authorization or [*9] exceeding authorized access" and thereby (i) obtaining information or (ii) obtaining any thing of value. 18 U.S.C. § 1030(a)(2)(C); § 1030(a)(4). The SCA prohibits "intentionally access[ing] without authorization a facility through which electronic communications are provided" or doing so in excess of authorization, and, in so doing, obtaining access to an electronic communication while it is in electronic storage. 18 U.S.C. § 2701(a). The relevant Virginia statute prohibits using a computer network "without authority" and thereby obtaining, embezzling, or converting property. ⁵ Va. Code § 18.2-152.3. Thus, common to all of these statutes is a prohibition against *unauthorized* access to a computer network, a violation of which triggers civil liability.

FOOTNOTES

⁵ Because the authorization element of the Virginia statute essentially parrots the relevant federal laws, the term is presumed to have the same meaning for purposes of both. See *Wilks v. Commonwealth of Va.*, 217 Va. 885, 234 S.E.2d 250, 251 (Va. 1977).

Mr. Yessin argues that these counts must be dismissed because there is no dispute that he was a manager of GPP during the relevant time period, and that as a manager, he was authorized as a matter of [*10] Florida law to access Mrs. Yessin's GPP e-mail account. In essence, he contends that Florida law allows a manager of a limited liability corporation unfettered access to the LLC's computer network, including the password-protected e-mail accounts of his co-managers. This argument fails.

^{HN2} Courts have generally and sensibly concluded that the scope of an individual's authorization to access a computer network is analyzed "on the basis of the expected norms of intended use." *United States v. Phillips*, 477 F.3d 215, 219 (5th Cir. 2007). ⁶ In other words, authorization to access a computer network may not, in some cases, turn simply on a person's status or position because the "expected norms of intended use" of the network may indicate otherwise. Accordingly, whether authorization existed may require a factual inquiry beyond the scope of the threshold motion stage. Indeed, in this case, it is clear from the complaint's allegations that the issue of authorization requires such an inquiry. Specifically, the factual allegations (i) that Mr. Yessin used a password to access an e-mail account that did not belong to him and (ii) that he lacked a legitimate business reason to do so are sufficient [*11] to create a plausible

inference that he acted without authorization within the meaning of the relevant statutes. See *A. V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 645 (4th Cir. 2009) (concluding that use of another's password to access website without website owner's permission was unauthorized access in violation of CFAA); *State Analysis, Inc. v. Am. Fin. Servs. Assocs.*, 621 F. Supp. 2d 309, 316 (E.D. Va. 2009) (same).

FOOTNOTES

⁶ By no means is the Fifth Circuit the only court of appeals to conclude that authorization is an intensely fact-driven analysis. Indeed, the circuits generally agree that the inquiry is primarily a factual one. See *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930 (9th Cir. 2004); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582 (1st Cir. 2001); *United States v. Morris*, 928 F.2d 504, 505 (2d Cir. 1991).

Moreover, Mr. Yessin cites no explicit Florida statute or case for the proposition that, as a matter of Florida law, he was authorized to access a fellow manager's GPP e-mail account by virtue of his status as a manager of GPP, an LLC. Instead, he cites only ^{HN3} Fla. Stat. § 608.4235, which, in the course of entitling managers to act as agents of [*12] an LLC for the purpose of carrying out the LLC's ordinary business, specifies that managers of LLC "may sign and deliver any instrument transferring or affecting the limited liability company's interest in real property." Fla. Stat. § 608.4235. This statute, for two reasons, does not bear the weight Mr. Yessin places on it. First, the statute concerns the power of managers to transfer title to real property, and it is difficult to comprehend what, if anything, this has to do with the alleged conduct at issue here, namely accessing password-protected data stored on a computer server. The statute does not address computer access. Second, it is clear that the provision clarifies and informs the scope of managers' power to act as agents in the ordinary course of the LLC's business. Yet, plaintiffs allege that Mr. Yessin had no legitimate business reason to access Mrs. Yessin's e-mail account and that he did so purely for personal gain. Thus, even assuming that Florida law might authorize managers to access information stored on an LLC's computer servers for purposes of carrying out the company's business, the factual allegations in the complaint are plainly sufficient to create a plausible [*13] inference that Mr. Yessin was not acting as an agent of GPP in accessing Mrs. Yessin's e-mail account. Accordingly, plaintiffs have asserted sufficient factual allegations to create a plausible inference that Mr. Yessin did not have authorization to access Mrs. Yessin's GPP e-mail account. Mr. Yessin's motion to dismiss these counts on the ground that he was so authorized is therefore appropriately denied.

B. Claims Alleging Unlawful Interception of Communications

In Counts 3, 4, 5, 8, 9, 10, and 11, plaintiffs allege that Mr. Yessin unlawfully "intercepted" Mrs. Yessin's e-mail communications, in violation of the interception provisions common to both the ECPA, 18 U.S.C. § 2511, and Va. Code § 19.2-62(A). Mr. Yessin argues that this allegation fails as a matter of law because no "intercept" occurs where, as alleged, the e-mail messages were accessed where they were stored on the destination server. He contends that a statutory intercept requires contemporaneous acquisition of the message at the time it is transmitted by the sender.

^{HN4} The ECPA, in pertinent part, prohibits intentionally intercepting any electronic communication. 18 U.S.C. § 2511(1)(a). The act further defines "intercept" [*14] to mean "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). The pertinent Virginia statute essentially parrots the federal statute. Compare Va. Code § 19.2-62(A) ("Any person who intentionally intercepts, endeavors to intercept or procures any other person to intercept or endeavor to intercept any wire, electronic, or oral communications . . .") with 18 U.S.C. § 2511(1) ("Any person who intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . ."). Indeed, the Supreme Court of Virginia has forthrightly stated that Va. Code § 19.2-62 "is Virginia's version" of the ECPA. And the Virginia Code defines "intercept" in terms virtually identical to the ECPA's definition. See Va. Code § 19.2-61 (defining "intercept" to mean "any aural or other means of acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical, or other device"). Thus, the term "intercept" in Va. Code § 19.2-62 is appropriately [*15] construed and applied in precisely the same way as its federal counterpart. ⁷

FOOTNOTES

⁷ Cf. *Wilks*, 234 S.E.2d at 252 (referring to definition of "oral communication" in ECPA case law to in order define the same phrase for purposes of Va. Code § 19.2-62).

^{HN5} Courts applying the ECPA have consistently held that a qualifying "intercept" occurs only where the acquisition of the communication occurs contemporaneously with its transmission by its sender. ⁸ Thus, interception includes accessing messages in transient storage on a server during the course of transmission, but does *not* include accessing the messages stored on a destination server. Compare *Hall v. EarthLink Network, Inc.*, 396 F.3d 500, 504 n.1 (2d Cir. 2005) (recognizing claim alleging interception of message while temporarily stored on server during transmission to destination server) with *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114 (3d Cir. 2003) (concluding that company did not intercept employee's e-mail by accessing messages stored on company server). In other words, these statutes give "intercept" its common meaning, which is perhaps best understood through a football analogy. In American football, a ball can only be intercepted [***16**] when it is "in flight." ⁹ Once a pass receiver on the offensive team has caught the ball, the window for interception has closed, and defenders can only hope to force a fumble. In essentially the same way, a qualifying "intercept" under the ECPA and Va. Code § 19.2-62 can only occur where an e-mail communication is accessed at some point between the time the communication is sent and the time it is received by the destination server, at which point it becomes a "stored communication" within the meaning of the SCA. Thus, accessing a stored communication does not constitute an "intercept" within the meaning of the ECPA or Va. Code § 19.2-62. See *supra* note 8. Plaintiffs' suggestion to the contrary would render redundant the "intercept" prohibitions of the ECPA and the "accessing stored communications" prohibitions of the SCA--an impermissible result given that the two laws were enacted as part of the same bill. See Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986); see also *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 877 (9th Cir. 2002) (concluding that "intercept" as defined in ECPA should be construed narrowly in light of separate "access" [***17**] provisions of SCA); *Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457, 461-62 (5th Cir. 1994) (same). ¹⁰

FOOTNOTES

⁸ See *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113-14 (3d Cir. 2003); *United States v. Steiger*, 318 F.3d 1039, 1048-49 (11th Cir. 2003); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878-79 (9th Cir. 2002); *Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457, 464 (5th Cir. 1994); see also *United States v. Councilman*, 418 F.3d 67, 79 (1st Cir. 2005) (concluding that copying e-mail messages from transient storage on Internet service provider server during course of transmission constituted "interception" within meaning of ECPA); *Hall v. EarthLink Network, Inc.*, 396 F.3d 500, 504 n.1 (2d Cir. 2005) (adopting contemporaneous transmission requirement but distinguishing case where Internet service provider received and stored, without forwarding, e-mail messages intended for plaintiff).

⁹ *Official Playing Rules and Casebook of the National Football League*, Rule 3, § 2, Art. 7 (2009) (defining "interception" and "catch").

¹⁰ For a contrary but unpersuasive view, see *Konop*, 302 F.3d at 889 (Reinhardt, J., dissenting) (arguing that "access" is best "understood as [***18**] being *qualitatively* different" from "intercept," i.e., as a lesser-included offense, and not *temporally* different). Notably absent from Judge Reinhardt's analysis is any explanation of *why* Congress would use the term "access" as a lesser-included offense to "intercept" when the common understandings of the terms do not reveal such a relationship.

These principles, applied here, point persuasively to the conclusion that the complaint's factual allegations do not support a plausible inference that Mr. Yessin "intercepted" communications intended for plaintiffs within the meaning of the ECPA or the Virginia Code. Nor have plaintiffs forecasted that there are any facts they can alleged that would remedy this fatal flaw. Indeed, plaintiffs allege that Mr. Yessin was stymied once Mrs. Yessin changed her e-mail account password, causing him to ask GPP's information technology consultant to give him Mrs. Yessin's password. This allegation is plainly inconsistent with a theory that Mr. Yessin somehow intercepted e-mail messages during their transmission and before they reached Mrs. Yessin's account on GPP's server. In response, plaintiffs assert that Mrs. Yessin had not yet read some of

the [*19] e-mail messages on the GPP server by the time. This allegation is irrelevant. Irrespective of whether Mrs. Yessin read the e-mail messages in question, they had reached their destination server. Accordingly, they were no longer in transmission by the time Mr. Yessin allegedly accessed them. ¹¹ Finally, in support of their argument that they have met their pleading burden, plaintiffs note that they use the word "intercepted" at least thirteen times in the complaint. Pls.' Mem. in Opp. at 25. Yet, the mere use of the word, even repeatedly, does not make it so. Instead, this is nothing more than a "threadbare recital[] of a cause of action's elements, supported by mere conclusory statements." *Iqbal*, 129 S. Ct. at 1940 (quoting *Twombly*, 550 U.S. at 555). Such recitations are not entitled to the presumption of truth accorded a complaint's factual allegations at the Rule 12 stage. Plaintiffs have therefore failed to allege facts that create a plausible inference that Mr. Yessin intercepted plaintiffs' communications. Accordingly, these counts must be dismissed.

FOOTNOTES

¹¹ Nor is the analysis any different for outgoing e-mails allegedly read by Mr. Yessin. When an e-mail message is sent, a copy will [*20] often be stored on the origin server. Mr. Yessin allegedly accessed these sent e-mails. Yet, these are merely stored copies of already-transmitted e-mails. Accordingly, they, too, were not intercepted within the meaning of the relevant statutes.

C. Claim Alleging Obtaining, Embezzlement, or Conversion of Property

Count 12 of the complaint alleges that Mr. Yessin obtained, embezzled, or converted property through unauthorized use of GPP's computer network in violation of ^{HN6} Va. Code § 18.2-152.3, creates a civil remedy against "any person who uses a computer or computer network, without authority and: (i) obtains property or services by false pretense, (ii) embezzles or commits larceny, or (iii) converts the property of another." The complaint alleges no facts suggesting that Mr. Yessin obtained, embezzled, or converted plaintiffs' property through his alleged use of GPP's computer network. Plaintiffs argue that Mr. Yessin's alleged act of surveilling Mrs. Yessin's e-mail itself was conversion of property within the meaning of the statute. Yet, there is simply no support--in the language of the statute or in the case law--for plaintiffs' argument that the mere act of reading an electronic [*21] communication constitutes conversion of property under § 18.2-152.3.

The only support plaintiffs cite for their expansive interpretation of the statute is *Barnes v. Commonwealth of Va.*, 2000 Va. App. LEXIS 204, at *1 (Va. Ct. App. Mar. 21, 2000). *Barnes* is plainly distinguishable from this case. In *Barnes*, the court concluded that unauthorized access to a Virginia motor vehicles database fell within the scope of the statute because the access was used to assist in the retention of a stolen car. *Id.* Thus, the access to the computer network in *Barnes* directly furthered the conversion of personal property, namely the car, and as such, this fell within the statute's scope. No such facts are alleged here; the purported access to the computer network was not in order to accomplish the conversion of property, but rather was in order to gain an advantage in divorce proceedings. On these alleged facts, a law prohibiting obtaining, embezzlement, or conversion of property simply does not apply. Accordingly, Mr. Yessin's motion to dismiss must be granted with respect to Count 12.

D. Claim Alleging Unauthorized Examination of Specified Personal Information

Count 13 alleges a violation of ^{HN7} Va. Code § 18.2-152.5, [*22] which prohibits unauthorized use of a computer network to examine employment, salary, credit, or other financial or identifying information. To state a valid claim under this statute, plaintiffs must allege facts creating a plausible inference that Mr. Yessin (i) used a computer or computer network (ii) without authority, (iii) with the intent to examine another's records, (iv) without authority, and (v) the records contained employment, salary, credit, or other financial or identifying information as defined by the statute. *S.R. v. INOVA Healthcare Servs.*, 49 Va. Cir. 119 (Fairfax Co. 1999). Thus, under *Iqbal*, plaintiffs must allege facts that, if true, create plausible inferences that these elements are satisfied. 129 S. Ct. at 1949.

The complaint fails to do so; it does not allege any facts concerning the content of the e-mail messages in issue other than that they contained sensitive information regarding Mrs. Yessin's legal strategy in the pending divorce proceeding. Because legal strategy does not fall into any of the statute's enumerated categories either literally or pursuant to *ejusdem generis*, this allegation is insufficient to sustain a claim of

a violation of § 18.2-152.5. [*23] Accordingly, Count 13 must be dismissed, but with leave to amend. If plaintiffs are able to amend their complaint, consistently with Rule 11, Fed. R. Civ. P., to include factual allegations concerning any personal information viewed by Mr. Yessin in violation of § 18.2-152.5, they may do so.

E. Whether GPP is Validly a Plaintiff in This Case

Mr. Yessin argues that GPP is not a party to this case because the company has not authorized this suit as required by Florida law. Specifically, Mr. Yessin argues that a meeting of the managers of GPP was required in order for this suit to be filed on GPP's behalf, and Mr. Yessin asserts that no such meeting occurred.

It is pellucidly clear that this argument fails at this stage of the proceeding. Plaintiffs dispute that Florida law requires a meeting in circumstances where a majority of the members of the LLC agree by written consent to the proposed action. Yet, even assuming, *arguendo*, that such a meeting was required, subsequent briefing reveals that plaintiffs contend that one was held. Thus, whether this action was properly authorized by GPP is clearly a factual dispute that, given the complaint's allegations, cannot be decided on a motion to [*24] dismiss. Accordingly, Mr. Yessin's motion to dismiss GPP as a party to the suit is appropriately denied at this time.

IV.

Finally, Mr. Yessin argues that this case should be stayed pending the outcome of a suit for declaratory relief he filed in Florida court subsequent to the commencement of this action. The relief defendant seeks in the Florida suit is a declaration that he is now the sole manager of GPP. Mr. Yessin's motion to stay this proceeding must be denied.

While it is true that the general interest in judicial economy favors avoiding duplicative litigation, that interest is not by any means unyielding and, in any event, the principle is not applicable where, as here, the other action is a second-in-time lawsuit governing a question that is only tangentially related to, but not dispositive of, the instant matter.¹² The Florida lawsuit seeks a declaration that Mr. Yessin is now the sole manager of GPP. While Mr. Yessin suggests that the outcome of the Florida proceeding could have a dispositive effect on this case, it is quite clear that it would have no such impact. Indeed, whether Mr. Yessin is now GPP's sole manager would appear to bear only on *one* element of *some* of the claims--specifically, [*25] whether Mr. Yessin was authorized to access GPP's computer network. Yet, as discussed above, a declaration that Mr. Yessin is now GPP's sole manager would not have a dispositive effect on the disputed "authorization" element, as it is quite possible that a trier of fact could conclude that Mr. Yessin, despite now being GPP's sole manager, was nonetheless not authorized to access Mrs. Yessin's e-mail for his personal benefit. See *supra* Part III.A. Thus, because Mr. Yessin has not shown sufficient good cause to stay these proceedings, the motion is appropriately denied.

FOOTNOTES

¹² See *Ulmet v. United States*, 888 F.2d 1028, 1035 (4th Cir. 1989). In *Ulmet*, the Fourth Circuit concluded that the "virtually unflagging obligation of the federal courts to exercise the jurisdiction given them" required that the district court hear a request for equitable relief despite a pending action in the United States Claims Court over the same claim. *Id.* (quoting *Colo. River Water Conservation Dist. v. United States*, 424 U.S. 800, 817, 96 S. Ct. 1236, 47 L. Ed. 2d 483 (1976)).

V.

In summary, Mr. Yessin's motion to dismiss must be granted in part and denied in part. It must be granted with respect to Counts 3, 4, 5, 8, 9, 10, and 11 because plaintiffs [*26] have not alleged facts creating a plausible inference that Mr. Yessin "intercepted" any communications, nor have they forecasted any factual allegations that would create such a plausible inference. Moreover, Mr. Yessin's motion must be granted with respect to Counts 12 and 13 because plaintiffs have neither alleged nor forecasted facts that would sustain a conclusion that Mr. Yessin examined certain sensitive information or obtained, embezzled, or converted any property. Count 13 is appropriately dismissed, but with leave to amend. But Mr. Yessin's motion is appropriately denied with respect to Counts 1, 2, 6, and 7 because plaintiffs have pleaded

sufficient facts to create a plausible inference that Mr. Yessin lacked authorization to access Mrs. Yessin's e-mail account. Moreover, whether GPP is validly a party to this suit is an issue that cannot properly be decided solely on the pleadings, as is required at the threshold motion stage. Finally, there is not good cause to stay this proceeding pending the outcome of the declaratory judgment suit action brought by Mr. Yessin in a Florida court.

The Clerk is directed to send a copy of this Memorandum Opinion to all counsel of record.

Alexandria, [*27] Virginia

November 24, 2009

/s/ T. S. Ellis, III ▾

T. S. Ellis, III ▾

United States District Judge

Source: [Legal](#) > / . . . / > **VA Federal District Courts** ⓘ

Terms: **name(global policy partners and yessin)** ([Edit Search](#) | [Suggest Terms for My Search](#))

View: Full

Date/Time: Tuesday, February 9, 2010 - 1:23 PM EST

[Search](#) | [Research Tasks](#) | [Get a Document](#) | [Shepard's®](#) | [Alerts](#) | [Total Litigator](#) | [Transactional Advisor](#) | [Counsel Selector](#)
[History](#) | [Delivery Manager](#) | [Dossier](#) | [Switch Client](#) | [Preferences](#) | [Sign Out](#) | [Help](#)



LexisNexis®

[About LexisNexis](#) | [Terms & Conditions](#) | [Contact Us](#)

Copyright © 2010 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.