

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MONTANA  
BILLINGS DIVISION**

**DALE MORTENSEN and MELISSA  
BECKER, individually, and on  
behalf of themselves and all others  
similarly situated,**

**Plaintiffs,**

**vs.**

**BRESNAN COMMUNICATION,**

**L.L.C.**

**Defendant.**

**CV 10-13-BLG-RFC**

**ORDER**

Presently before the Court is Defendant Bresnan Communications, LLC's ("Bresnan") Motion to Dismiss pursuant to Fed.R.Civ.P. 12(b)(6). *Doc. 10*. In bringing the motion, Bresnan contends that Plaintiffs present claims fail to state a claim upon which relief may be granted (1) under the Electronic Communications Privacy Act ("ECPA"); (2) under Computer Fraud and Abuse Act ("CFAA"); (3)

for invasion of privacy; and (4) for trespass to chattel. Plaintiffs oppose the motion.

## **BACKGROUND**

This is a class action suit. Plaintiffs, representing a putative class, allege that from early 2008 through June of 2008, Defendant Bresnan Communications, as an Internet Service Provider (“ISP”), diverted substantially all of Plaintiffs’ Internet communications to NebuAd, Inc., a third-party Internet advertising company. Plaintiffs allege that Bresnan allowed NebuAd to install its “Appliance” onto Bresnan’s network. Plaintiffs further allege that NebuAd used this Appliance to gather information to create profiles of Bresnan’s customers in order to target them with preference-sensitive advertisement. In addition, Plaintiffs allege that Bresnan profited from the alleged invasion.

Plaintiffs contend that these activities were not in Bresnan’s regular course of business as an ISP and were not to protect Bresnan or its customers. Moreover, Plaintiffs contend Bresnan never obtained the consent of its customers to perform this action. As such, Plaintiffs allege the following causes of action (1) violations of the Electronic Communications Privacy Act (“ECPA”); (2) violations of the Computer Fraud and Abuse Act (“CFAA”); (3) invasion of privacy; (4) unjust enrichment; and (5) trespass to chattel.

## **STANDARD OF REVIEW**

A Rule 12(b)(6) dismissal may be based on either a “lack of a cognizable legal theory or the absence of sufficient facts alleged under a cognizable legal theory.” *Johnson v. Riverside Healthcare System, LP*, 534 F.3d 1116, 1121-22 (9th Cir.2008). In other words, the plaintiff’s complaint must provide a “short and plain statement of the claim showing that [he] is entitled to relief.” *Johnson*, 534 F.3d at 1122. “Specific facts are not necessary; the statement need only give the defendant [s] fair notice of what ... the claim is and the grounds upon which it rests.” *Erickson v. Pardus*, 551 U.S. 89, 93 (2007).

Every complaint must, at a minimum, plead “enough facts to state a claim for relief that is plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007); *Weber v. Dept. of Veterans Affairs*, 521 F.3d 1061, 1065 (9th Cir.2008). Facts which are alleged in the complaint are presumed true, and the Court must construe them and draw all reasonable inferences from them in favor of the plaintiff. *Cahill v. Liberty Mutual Ins. Co.*, 80 F.3d 336, 337-38 (9th Cir.1996).

Nevertheless, and in spite of the deference the Court is bound to pay to any factual allegations made, it is not proper for the Court to assume that “the [plaintiff] can prove facts which [he or she] has not alleged.” *Associated General*

*Contractors of California, Inc. v. California State Council of Carpenters*, 459 U.S. 519, 526 (1983). Nor must the Court “accept as true allegations that contradict matters properly subject to judicial notice or by exhibit” or those which are “merely conclusory,” require “unwarranted deductions” or “unreasonable inferences.” *Sprewell v. Golden State Warriors*, 266 F.3d 979, 988 (9th Cir.2001) (*amended on other grounds*, 275 F.3d 1187 (9th Cir.2001)); *see also Iletto v. Glock Inc.*, 349 F.3d 1191, 1200 (9th Cir.2003) (court need not accept as true unreasonable inferences or conclusions of law cast in the form of factual allegations).

## **DISCUSSION**

Bresnan seeks dismissal of Plaintiffs’ claims pursuant to Fed.R.Civ.P. 12(b)(6).

### **A. *Electronic Communications Privacy Act (“ECPA”)***

Bresnan seeks dismissal of Plaintiffs’ claim under the ECPA (also known as Wiretap Act) that it violated the ECPA’s prohibition on intercepting, endeavoring to intercept and/or procuring interceptions (by NebuAd) of electronic communications as well as using and/or endeavoring to use electronic communications. 18 U.S.C. §§ 2511(1)(a) & 2511(1)(d).

**1. *Bresnan did not “intercept” an electronic communication***

Bresnan contends that it cannot be “liable for another’s interception or use of electronic communications.”<sup>1</sup> Specifically, Bresnan cites cases wherein liability under the ECPA cannot attach where a defendant acquiesces, has passive knowledge of, or instructs another to intercept or use electronic communications. *Reynolds v. Spears*, 93 F.3d 428, 432-33 (9th Cir. 1996); *Perkins-Carrillo v. Systemax*, 2006 WL 1553957, \*15 (N.D.Ga. 2006). In *Spears*, the Eighth Circuit Court found that the wife of a co-defendant was not liable under the ECPA just because she was aware, acquiesced and had passive knowledge of her husband’s unlawful interceptions. *Spears*, 93 F.3d at 433. In *Systemax*, the district court found that the ECPA attaches only to the individual or entity that engaged in the violation of interception, disclosure and intentional use and not to one that instructs the interception. *Id.*, 2006 WL 1553957 at 15.

Bresnan goes on to cite numerous other cases across the country to support its contention that it was nothing more than a passive conduit for NebuAd’s interception of Plaintiffs’ personal information. However, Plaintiffs have alleged in their Complaint that Bresnan allowed NebuAd to install its device (“Appliance”) on Bresnan’s network. Further, but for that Appliance, NebuAd

---

<sup>1</sup>DEFENDANT’S BRIEF IN SUPPORT OF MOTION TO DISMISS (Doc. #11) at p. 17.

would have been unable to access Plaintiffs' personal electronic transmissions.

Title I of the ECPA, the Wiretap Act makes it an offense to “intentionally intercept [ ] ... any wire, oral, or electronic communication.” 18 U.S.C. § 2511(1)(a). The Ninth Circuit's interpretation of the word “intercept” also comports with the ordinary meaning of the word, which is “to stop, seize, or interrupt in progress or course before arrival.” *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9<sup>th</sup> Cir. 2002)(quoting *Webster's Ninth New Collegiate Dictionary* 630 (1985)).

Here, the Class Action Complaint alleges that NebuAd and Bresnan deployed the Appliance on Bresnan's network infrastructure and configured its network to “funnel all User Internet through the Appliance.”<sup>2</sup> Further, the Complaint alleges that Bresnan maintained the Appliance and directed the flow of Plaintiffs' Internet traffic through the Appliance.<sup>3</sup>

Based on this, Plaintiffs have pled sufficient facts to establish, for purposes of a 12(b)(6) motion to dismiss, that Bresnan intercepted Plaintiffs' electronic communications in violation of the ECPA. Bresnan's Motion to Dismiss on this ground is DENIED.

---

<sup>2</sup>CLASS ACTION COMPLAINT (Doc. #1), ¶ 20.

<sup>3</sup>Id., at ¶ 21.

**2. *Plaintiffs consented to the interception***

In the alternative, Bresnan argues that Plaintiffs agreed to the interception when they agreed to the terms of using Bresnan's Internet service and thus consented to all acts alleged in the Class Action Complaint.

An intentional interception of a telephone conversation is not actionable if a party to the conversation gives prior consent to the interception. 18 U.S.C. § 2511(2)(d). "In the Title III milieu as in other settings, consent inheres where a person's behavior manifests acquiescence or a comparable diminution of his or her otherwise protected rights." *Griggs-Ryan v. Smith*, 904 F.2d 112, 116 (1st Cir.1990). A court can infer implied consent when the circumstances indicate that the party knowingly agreed to the surveillance. *United States v. Amen*, 831 F.2d 373, 378 (2d Cir.1987). Consent need not be explicit, but may be implied from "actual notice" of the interception. *Amati v. City of Woodstock*, 176 F.3d 952, 955 (7<sup>th</sup> Cir. 1999)

Bresnan argues that even if it had intercepted an electronic communication, Plaintiffs had consented to the interception in the *Bresnan Communications OnLine Privacy Notice* and in Bresnan's *OnLine Subscriber Agreement*.<sup>4</sup> A

---

<sup>4</sup>*DEFENDANT'S BRIEF IN SUPPORT OF MOTION TO DISMISS (Doc. #11), Exhibits C & D, respectively.*

review of these documents informs Bresnan's customers that they agree to allow Bresnan and its agents to monitor electronic postings and transmissions as well as use equipment to collect information on Plaintiffs' Internet usage.<sup>5</sup> Specifically, Defendant Bresnan's *Online Privacy Notice* informed the Plaintiffs that when using Bresnan's Service,

the Service equipment automatically collects information on your use of the Service including information on the choices that you make along the range of services offered, the programs and web sites you review or services you order, the time that you actually use the Service or view the programs and web sites, other information about your 'electronic browsing,' and the text of e-mail or other electronic communications you send or receive using any of these services.

\* \* \*

In addition, when you use the Service or any Internet service, certain information relating to your use of these services may be disclosed to third parties that provide content or services. Such disclosure may include, without limitation, information on the choices that you make along the range of services offered, including the content, programs and web sites you view or services you order on the Service or on the Internet, the time that you actually use the services or view the content and web sites, and other information about your "electronic browsing."

\* \* \*

From time to time, Bresnan Communications may engage reliable third parties to provide, license or sublicense goods or services . . . to its subscribers. . . Such third parties may collect and generate information concerning customers or subscribers in the course of providing services to them.

Bresnan Communications will provide such third parties with subscriber information necessary to provide the Third-Party Services and may grant to

---

<sup>5</sup>Id.



such third parties the right to access and use such subscriber information for billing, support, network monitoring and planning, and to otherwise fulfill such third party's obligations to Bresnan Communications and/or the Service and their respective subscribers.<sup>6</sup>

In Bresnan's *OnLine Subscriber Agreement*, Bresnan informed its customers regarding,

(g.) ***Monitoring of Postings and Transmissions.*** Bresnan Communications shall have no obligation to monitor postings or transmissions made in connection with the Service. However, Customer acknowledges and agrees that Bresnan Communications and its agents shall have the right to monitor any such postings and transmissions, including without limitation email, newsgroups, chat, IP audio and video, and web space content, from time to time and to disclose them in accordance with the terms of this Agreement, applicable law or government request.<sup>7</sup>

Finally, Bresnan contends that it gave Plaintiffs specific notice of when the NebuAd Appliance trial would commence and provided a link for its customers to opt out of the NebuAd Appliance if they so chose.<sup>8</sup>

Significantly, Plaintiffs do not contest that they agreed, by way of Bresnan's *Privacy Notice and Subscriber Agreement*, to the interception. Rather, Plaintiffs argue Bresnan construed their consent too broadly and that Bresnan "cavalierly" implied the Plaintiffs' consent. *Watkins v. Berry*, 704 F.2d 577, 581 (11th

---

<sup>6</sup>DEFENDANT'S BRIEF IN SUPPORT OF MOTION TO DISMISS (Doc. #11), Exhibit C

<sup>7</sup>DEFENDANT'S BRIEF IN SUPPORT OF MOTION TO DISMISS (Doc. #11), Exhibit D

<sup>8</sup>DEFENDANT'S BRIEF IN SUPPORT OF MOTION TO DISMISS (Doc. #11), Exhibit E.

Cir.1983). According to Plaintiffs, they were not aware of the monitoring and therefore could not consent in fact. Plaintiffs contend that Bresnan did not obtain meaningful consent for the interception in that it did not fully describe its intent to funnel “customer’s complete, unfiltered Internet traffic to a third-party processor for profiling and ad-serving.”<sup>9</sup> Finally, Plaintiffs note Bresnan could have explained the privacy protections and revenue benefits at issue as well as obtaining opt-in consent prior to commencement of the NebuAd Appliance trial.

“Without actual notice, consent can only be implied when the surrounding circumstances convincingly show that the party knew about and consented to the interception.” *Berry v. Funk*, 146 F.3d 1003, 1011 (D.C.Cir.1998). In other words, someone who makes calls despite knowledge that they are being intercepted is considered to have consented to the interception. *U.S. v. Van Poyck*, 77 F.3d 285, 292 (9th Cir.1996). The *Griggs-Ryan* Court noted that,

implied consent is “consent in fact” which is inferred “from the surrounding circumstances indicating that they knowingly agreed to the surveillance.” Thus, implied consent-or the absence of it-may be deduced from the circumstances prevailing” in a given situation. The circumstances relevant to an implication of consent will vary from case to case, but the compendium will ordinarily include language or acts which tend to prove (or disprove) that a party knows of, or assents to, encroachments on the routine expectation that conversations are private. *Id.*,904 F.2d at 116-117.

---

<sup>9</sup>PLAINTIFFS’ OPPOSITION TO DEFENDANT’S MOTION TO DISMISS (Doc. #23) at 14.

Bresnan contends that it gave Plaintiffs specific notice of when the NebuAd Appliance trial would commence. Bresnan further contends that it provided a link for its customers to opt out of the NebuAd Appliance if they so chose. *United States v. Van Poyck*, 77 F.3d 285, 292 (9th Cir.1996); *United States v. Staves*, 383 F.3d 977, 981 (9th Cir.2004). Here, it appears that circumstances “indicate that [the] party to the communication knew that interception was likely and agreed to the monitoring.” *Staves*, 383 F.3d at 981.

This Court finds Plaintiffs’ argument to be without merit. As noted in Bresnan’s *Privacy Notice* and *OnLine Subscriber Agreement*, it is evident that Plaintiffs’ electronic transmissions would be monitored and would in fact be transferred to third-parties for the purposes of providing “content or services.”<sup>10</sup> Moreover, Bresnan provided Plaintiffs with specific notice of the NebuAd Appliance trial on its website. Consequently, there were at least three separate occasions where Bresnan informed Plaintiffs of its monitoring and possible transmission of Plaintiffs’ electronic activities to a third-party. Lastly, Bresnan’s *OnLine Subscriber Agreement* specifically states that “[p]lease read this Agreement very carefully, because by accepting the Service, you agree to all of

---

<sup>10</sup>DEFENDANT’S BRIEF IN SUPPORT OF MOTION TO DISMISS (Doc. #11), Exhibit C.

these terms.”<sup>11</sup>

For those reasons, the Court concludes that through the *OnLine Subscriber Agreement*, the *Privacy Notice* and the NebuAd link on Brenan’s website, Plaintiffs did know of the interception and through their continued use of Bresnan’s Internet Service, they gave or acquiesced their consent to such interception. *In re DoubleClick Inc. Privacy Litigation*, 154 F.Supp.2d 497, 514 (S.D.N.Y.2001).

Accordingly, Bresnan’s Motion to Dismiss the Plaintiffs’ ECPA claim is GRANTED.

**B. *Invasion of Privacy***

Next, Bresnan seeks dismissal of Plaintiffs’ common-law tort claim of invasion of privacy. Plaintiffs allege that by monitoring and transmitting Plaintiffs’ electronic communication, Bresnan wrongful intruded into Plaintiffs’ “private activities in such a manner as to outrage or cause mental suffering, shame or humiliation to a person of ordinary sensibilities.” *Deserly v. Department of Corrections*, 298 Mont. 328, 335 (2000) (citing *Sistok v. Northwestern Tel. Sys. Inc.*, 189 Mont. 82, 92 (1980)). Plaintiffs are alleging the invasion of privacy category of “intrusion upon seclusion.” To prevail on the tort of intrusion upon

---

<sup>11</sup>DEFENDANT’S BRIEF IN SUPPORT OF MOTION TO DISMISS (Doc. #11), Exhibit D.

seclusion, a plaintiff must show: (a) an actual, subjective expectation of seclusion or solitude, and (b) that the expectation was objectively reasonable. *Medical Lab. Mgmt. Consultants v. ABC*, 306 F.3d 806 (9th Cir.2002). A review of the Class Action Complaint adequately reflects Plaintiffs' subjective expectation of seclusion.

However, as noted earlier, the *Subscriber Agreement* and the *Privacy Notice* informed the Plaintiffs of the monitoring of their electronic communications and activities through the use of Bresnan's Internet service and network. Those documents further informed Plaintiffs of the potential that their electronic transmissions may be provided to a third-party for purposes of providing content or services. In addition, Plaintiffs were informed that the use of Bresnan's Service constituted acceptance of the terms of the *Subscriber Agreement* and *Privacy Notice*.

Under these facts, Plaintiffs cannot demonstrate that their expectation of privacy was objectively reasonable. *Miller v. Great Falls Athletic Club, LLC*, 2010 WL 3122633 at 2 (Mont. 2010); *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir.2004) (stating that individuals may not reasonably expect privacy in transmissions over the internet). Regardless of any subjective expectation of privacy, given Plaintiffs' notice of the monitoring and potential forwarding of

their electronic activities to a third-party, they did not have an objectively reasonable expectation of privacy. In addition, Plaintiffs were given specific notice of the NebuAd Appliance trial and were given an opportunity to opt out if they chose.<sup>12</sup> *United States v. Heckenkamp*, 482 F.3d 1142, 1147 (9th Cir. 2007) (“privacy expectations may be reduced if the user is advised that information transmitted through the network is not confidential and that the systems administrators may monitor communications transmitted by the user”).

Further, Plaintiffs, by using Bresnan’s Internet service, consented to Bresnan’s monitor and use of Plaintiffs’ electronic communications. *State v. Brubaker*, 184 Mont. 294, 301 (1979) (although discussing the heightened constitutional right to privacy, the Montana Supreme Court stated that once a person voluntarily consents to an invasion, his constitutional right to privacy disappears). For the foregoing reasons, this Court concludes that Plaintiffs have failed to meet the objective prong of intrusion upon seclusion. Bresnan’s Motion to Dismiss on Plaintiffs’ invasion of privacy claim is therefore GRANTED.

---

<sup>12</sup>Bresnan argues, with some merit, that it is the intrusion onto the privacy that gives rise to the cause of action of invasion of privacy and not the subsequent disclosure of the private information. *Browning v. AT&T Corp.*, 682 F.Supp.2d 832 (N.D. Ill. 2009). Here, the crux of Plaintiffs’ claims are that their injuries arise not from the interception of their electronic communications, but the disclosure of said communications to a third-party.

**C. *Computer Fraud and Abuse Act***

Next, Bresnan seeks dismissal of Plaintiffs' claim that it violated the Computer Fraud and Abuse Act ("CFAA") when it accessed Plaintiffs' computers without authorization and caused Plaintiffs to suffer damages/loss.

The CFAA prohibits any person from intentionally accessing a computer without authorization or exceeding authorized access, and thereby obtain information from any protected computer. 18 U.S.C. § 1030(a)(2)(C). The CFAA also prohibits any person from intentionally accessing a protected computer without authorization, and as a result of such conduct, causing damage and loss. 18 U.S.C. §§ 1030(a)(5)(B)& (C). The CFAA defines "exceeds authorized access" as "access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled to so obtain or alter." 18 U.S.C. § 1030(e)(6); *see also LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1132-33 (9th Cir.2009) (discussing "authorization" under the CFAA). Although a criminal statute, 18 U.S.C. § 1030(g) allows for right of action for private persons injured under the CFAA.

Thus, to bring a claim under 18 U.S.C. §1030(a), Plaintiffs must show that Bresnan: (1) intentionally accessed a computer, (2) without authorization or exceeding authorized access, and (3) thereby obtained or altered information (4)

from any protected computer and that (5) there was loss to one or more persons during any one-year period aggregating at least \$5,000 in value. *Id.*; *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1132 (9th Cir. 2009).

**1. Damage and Loss**

Bresnan argues that dismissal of Plaintiffs' CFAA claim is appropriate because, other than conclusory allegations that mirror the CFAA statute, Plaintiffs have failed to allege any specific damages or loss in excess of \$5,000.

The CFAA defines "damage" as "any impairment to the integrity or availability of data, a system, or information." 18 U.S.C. § 1030(e)(8). Under the CFAA, "loss" is treated differently from "damage," and is defined as: "[a]ny reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11). Accordingly, Plaintiffs must claim economic loss or damages in an amount "aggregating at least \$5,000 in value during any 1-year period to one or more individuals." See 18 U.S.C. § 1030(e)(8)(A).

Insofar as Plaintiffs allege they suffered emotional distress due to Bresnan's invasion of their privacy, trespass to chattel, and any misappropriation of



confidential data, their injuries are not actionable because only economic losses are recoverable under the CFAA. *Letscher v. Swiss Bank Corp*, 1996 WL 183019, at \*2 (S.D.N.Y. 1996); *see also S. Rep No. 101-544* (1990) (“Damages [under § 1030(e)(8) (A) ] are limited to economic damages, except for violations of the medical records section, when pain and suffering damages would be permitted.”)

Here, Plaintiffs contend they have suffered loss and damages that exceed \$5,000. Specifically, they argue that Bresnan allowed the NebuAd Appliance to disable and alter Plaintiffs’ security features on their computers in order to place its “cookies” to track Plaintiffs’ Internet activities. Further, Plaintiffs contend they were forced to mitigate Bresnan’s invasive actions by expending time, money and resources to investigate and repair their personal computer’s diminished performance.

In opposition to Bresnan’s dismissal motion, Plaintiffs rely on *In re Toys R Us, Inc., Privacy Litigation*, 2001 WL 34517252 (N.D.Cal. 2001). In that case, that court found that plaintiffs had met the \$5,000 loss requirement under the CFAA because defendants caused identical cookies to be placed on plaintiff’s computers, unbeknownst to them. Contrary to Bresnan’s argument, these identical files or “cookies” implanted on each of plaintiff’s computers resulting in damages of a uniform nature. *Id.* As such, the *Toys R Us* court found that plaintiffs could

aggregate their damages and therefore had sufficiently pled the existence of a single act resulting in damages exceeding \$5,000 during any one-year period to one or more individuals. *Id.*, 2001 WL 34517252 at 11; *see also In re Apple & AT & TM Antitrust Litigation*, 596 F.Supp.2d 1288, 1308 (N.D.Cal. 2008).

It is evident in review of the case law, that damages and loss under the CFAA focuses on the Bresnan's act of distribution of the "cookie" or in this instance, Bresnan's single act of installing and distributing the NebuAd Appliance. Given that the NebuAd Appliance was distributed to all Plaintiffs, for purposes of a 12(b)(6) motion, Plaintiffs' allegations of the above-stated damages, when aggregated across "one or more individuals" is sufficient to survive a dismissal motion. *Id.* Bresnan's Motion to Dismiss on this Ground is therefore DENIED.

## **2. Authorization**

Plaintiffs have alleged that Bresnan, in violation of the CFAA, intentionally placed the NebuAd Appliance and its "cookies" on Plaintiffs' computers. The "cookies" allegedly allowed NebuAd, through the Bresnan, to retrieve data from Plaintiffs' computers. Plaintiffs allege that Bresnan placed the cookies on the computers and retrieved the data for the purpose of monitoring Plaintiffs' web activity. In response, Bresnan contends that Plaintiffs, through their use of its Internet service, consented and authorized Bresnan's access to Plaintiffs'

computers.

“[A] person uses a computer ‘without authorization’ under § 1030(a)(2) and (4) when the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway.” *LVRC Holdings*, 581 F.3d at 1135.

The Court, as stated above, has concluded that Plaintiffs’ use of Bresnan’s Internet service constituted acceptance of the terms of Bresnan’s *Privacy Notice* and *OnLine Subscriber Agreement*. The terms of those agreements reflect that Plaintiffs consented and authorized Bresnan’s monitoring of Plaintiffs’ electronic communications and activities. Further, by use of Bresnan’s Internet service, Plaintiffs were informed of the potential that their electronic transmissions may be provided to a third-party for purposes of providing content or services. As such, for purposes of the CFAA, this Court concludes that Bresnan did not access Plaintiff’s computers “without authorization.”

The next issue is whether Bresnan has “exceeded authorization.” Here, Plaintiffs argue that the NebuAd Appliance, which Bresnan allowed to access Plaintiffs’ computers, altered the character of Plaintiffs’ computers’ privacy and

security control protocols.

A reading of Bresnan's *Privacy Notice* and *OnLine Subscriber Agreement* as well as the NebuAd Appliance trial weblink provide no notice to Plaintiffs that their computer settings were to be actively altered or tampered with by Bresnan. To the extent Bresnan argues that it was NebuAd that exceeded the authorized access, Plaintiffs' allegations are sufficient to presume that Bresnan acted in concert with NebuAd by installing the Appliance onto its network. These present allegations run contrary to Bresnan's argument that its actions are nothing more than that of a passive party that monitors and provides Plaintiffs' electronic information to a third-party for purposes of providing services or content. For purposes of a 12(b)(6) motion, Plaintiffs have sufficiently alleged that Bresnan's act of tampering with the security and privacy protocols exceeded any authorization that Plaintiffs may have given. Bresnan's Motion to Dismiss Plaintiffs' CFAA claim is DENIED.

**D. *Trespass to Chattel***

Finally, Bresnan seeks dismissal of Plaintiffs' claim of trespass to chattel. This Court notes that Montana case law has limited recognition, if at all, of this common-law tort claim. As such, this Court must look to other states. Trespass to chattels "lies where an intentional interference with the possession of personal

property has proximately cause injury.” *Thrifty-Tel v. Bezenek*, 54 Cal.Rptr.2d 468 (1996). In order to prevail on a claim for trespass based on accessing a computer system, the plaintiff must establish: (1) defendant intentionally and without authorization interfered with plaintiff's possessory interest in the computer system; and (2) defendant's unauthorized use proximately resulted in damage to plaintiff. *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F.Supp.2d 1058, 1069 (N.D.Cal. 2000); *See Thrifty-Tel*, 54 Cal.Rptr.2d 468.

In the instant case, it is undisputed that Plaintiffs' personal computers are private property. By way of agreements with Bresnan and use of Bresnan's ISP, Plaintiffs have granted Bresnan conditional access for purposes of monitoring Plaintiffs' electronic transmissions as well as placing "cookies" on Plaintiffs' computers for purposes of tracking web activity. However, like Plaintiffs' CFAA claim, Bresnan's alleged actions of altering the privacy and security controls on Plaintiffs' computers activity is sufficiently outside of the scope of the use permitted by Plaintiffs. As such, for purposes of a 12(b)(6) motion, Plaintiffs have sufficiently alleged that Bresnan intentionally interfered with the possession of their personal property. Bresnan's Motion to Dismiss Plaintiffs' trespass to chattel claim is DENIED.

**CONCLUSION**

As reflected above, Bresnan's Motion to Dismiss Plaintiffs' claim under the Electronic Communications Privacy Act ("ECPA") is GRANTED. Bresnan's Motion to Dismiss Plaintiffs' claim for invasion of privacy is GRANTED. Bresnan's Motion to Dismiss Plaintiffs' claim under Computer Fraud and Abuse Act ("CFAA") is DENIED. Bresnan's Motion to Dismiss Plaintiffs' claim for trespass to chattels is DENIED.

For the foregoing reasons, IT IS HEREBY ORDERED that Bresnan's Motion to Dismiss (*Doc. 10*) is GRANTED IN PART and DENIED IN PART.

DATED this 13<sup>th</sup> day of December, 2010.

*/s/ Richard F. Cebull*  
\_\_\_\_\_  
RICHARD F. CEBULL  
UNITED STATES. DISTRICT JUDGE