IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF PENNSYLVANIA

KATE GOSSELIN, Plaintiff, v. JONATHAN K. GOSSELIN, ROBERT HOFFMAN, and JOHN AND JANE DOES 1-20 Defendants.	)	CIVIL ACTION NO.: 13:4989 JURY TRIAL DEMANDED

DEFENDANT JONATHAN K. GOSSELIN'S BRIEF IN SUPPORT OF MOTION TO DISMISS

Defendant Jonathan K. Gosselin ("Jon", "Jonathan," or "Defendant"), by and through his attorneys, BrittonTuma and Orwig Law Offices, files *Defendant Jonathan K. Gosselin's Brief in Support of Motion to Dismiss.*

I. STATEMENT OF RELEVANT FACTS

On June 12, 1999, Jonathan K. Gosselin and Katie I. Gosselin ("Kate") were married. Kate is a registered nurse, last working in the nursing industry in December 2006. Jonathan is a Microsoft Certified Systems Engineer, last working in the information technology industry in November 2007, as an information technology analyst for the Pennsylvania Governor's Office.

While married, Jonathan and Kate lived together in the same home. In their home was a Dell desktop computer (the "Dell Computer") that Jonathan purchased in 2002, which is licensed to Jonathan Gosselin. The Dell Computer had a Microsoft Windows XP operating system and Microsoft Office software, both of which were licensed to Jonathan Gosselin. Jonathan Gosselin was always the Administrator of the Dell Computer; Kate was only a Power User and had no administrative permissions. Jonathan's Dell Computer eventually became the Gosselin family computer and the children began playing on it using either Jonathan's account or Kate's account.

Jonathan regularly backed up the hard drive of the Dell Computer and the backups were saved to CD ROM or DVD disks. The backups included .pst files containing Personal Folders belonging to Jonathan Gosselin and Kate Gosselin which were stored in the Microsoft Outlook email program under the following directory: C:/Documents and Settings/outlook.

On June 22, 2009, Kate filed for divorce. After Kate filed for divorce, Jonathan moved out of the family home and into an apartment above the garage of the family home (the "Apartment"); Jonathan left the Dell Computer in the family home for continued use by his children. Jonathan was still permitted access to the family home during this time. On or about April 2010, Jonathan observed the hard drive of the Dell Computer was failing so he performed a backup of it and stored the data on DVD disks. Jonathan created two copies of the DVDs, one for himself and one for Kate. These final backup DVDs included family pictures, business contracts, and other information. The backup DVDs were labeled and dated for archiving purposes.

Once the divorce was final, Jonathan was required to move from the Apartment; Kate continued living in the family home. When Jonathan moved from the Apartment, he left Kate's copy of the backup DVDs in the Apartment in a box along with other items he believed Kate would want. He informed Kate that the DVDs were in the box. The following day Kate called Jonathan and asked if he would be returning for any other items left in the Apartment and he responded that he was not and she could discard the items as she saw fit. The children told Jonathan that Kate (and a friend of hers) threw away in the trash everything left behind in the Apartment. Jonathan has not wrongfully access any computer, online accounts, or telephone belonging to Kate—it is far more plausible that Kate herself threw out the DVDs in the trash.

Shortly thereafter, the hard drive of the Dell Computer failed. Jonathan destroyed that hard drive in a manner consistent with his training by taking it apart, removing the physical disk,

physically destroying the physical disk, and then discarding the pieces away separate from the actual hard drive device.

II. ARGUMENTS AND AUTHORITIES

A. The Complaint Fails To Meet The Minimum Legal Standards Required To Survive A Rule 12(b)(6) Motion To Dismiss.

1. Plaintiff's Complaint consists of little more than threadbare recitals of the elements of causes of action and conclusory statements, which are insufficient to survive a motion to dismiss.

Federal Rule of Civil Procedure 12(b)(6) provides that a complaint must be dismissed if it fails to state a claim upon which relief can be granted. While a court considering a motion to dismiss is required to review the complaint in the light most favorable to the plaintiff, there are minimal standards that must be met. Conclusory allegations, legal conclusions couched as factual allegations, or mere recitation of the elements of a cause of action, are not entitled to such presumption.

Even under the liberal notice pleading requirements of Rule 8, a plaintiff must provide sufficient factual allegations to demonstrate a plausible claim for relief prior to the court unlocking the doors to expensive discovery. "[T]he pleading standard Rule 8 announces does not require 'detailed factual allegations,' but it demands more than an unadorned, the-defendant-unlawfully-harmed-me accusation." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555-56, (2007)).

In *Iqbal*, the Supreme Court provided a concise guide with three steps for courts to follow when considering a motion to dismiss. The Court makes a key distinction between what it calls "conclusory allegations" and "factual allegations" and treats them very differently. *Iqbal*, 556 U.S. at 680-81. The Court began its analysis with what is often referred to as "the two-pronged approach" set forth in *Twombly*, 550 U.S. at 556, and expounded upon it to further explain the steps for reviewing a motion to dismiss: (1) reject the "bald allegations" because bald allegations

are conclusory and not entitled to be assumed true; (2) considering only the "factual allegations," use common sense and judicial experience to consider the plausibility of the allegations and whether there is an "obvious alternative explanation." *See id.* at 679-82.

a) Reject the "bald allegations" because "bald allegations" are conclusory and not entitled to be assumed true.

In *Iqbal* the Court explained the principles for why the "bald allegations" must be rejected. "First, the tenet that a court must accept as true all of the allegations contained in a complaint is inapplicable to legal conclusions. Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Id.* at 678. Rule 8 does not unlock the doors of discovery for a plaintiff armed with nothing more than conclusions. *Id.* at 678-79.

Reviewing the complaint at issue in *Iqbal*, the Court stated "[w]e begin our analysis by identifying the allegations in the complaint that are not entitled to the assumption of truth." *Id.* at 680. The Court then looked at the following allegations: (1) "petitioners 'knew of, condoned, and willfully and maliciously agreed to subject [him]' to harsh conditions of confinement 'as a matter of policy, solely on account of [his] religion, race, and/or national origin and for no legitimate penological interest.'" (2) "Ashcroft was the 'principal architect' of this invidious policy, and [] Mueller was 'instrumental' in adopting and executing it." *Id.* at 680-81. The Court referred to these as "bare assertions, much like the pleading of conspiracy in *Twombly*, amount[ing] to nothing more than a 'formulaic recitation of the elements' of a constitutional discrimination claim, namely, that petitioners adopted a policy '"because of," not merely "in spite of," its adverse effects upon an identifiable group.' As such, the allegations are conclusory and not entitled to be assumed true." *Id.* at 681.

The Court made it very clear, however, that it was "not reject[ing] these bald allegations on the ground that they are unrealistic or nonsensical." *Id.* Instead, "[i]t is the conclusory nature

of [the] allegations rather than their extravagantly fanciful nature, that disentitles them to the presumption of truth." *Id.* In other words, the Court declared war on "bald allegations" because of their conclusory nature.

b) Considering only the "factual allegations," use common sense and judicial experience to consider the plausibility of the allegations and whether there is an "obvious alternative explanation."

Next consider only the "factual allegations" in the complaint to determine if they plausibly suggest an entitlement to relief. *Id.* at 681. "Determining whether a complaint states a plausible claim for relief will . . . be a context-specific task that requires the reviewing court to draw on its judicial experience and common sense. But where the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct, the complaint has alleged—but it has not 'show[n]'—'that the pleader is entitled to relief.'" *Iqbal*, 556 U.S. at 679.

The complaint in *Iqbal* contained "factual allegations" that, taken as true, were consistent with the plaintiff's claim for relief but that was not the end of analysis. There were more likely explanations which explained those events in a way that made the "factual allegations" not plausible. The plausibility requirement is what made the difference between granting and denying the motion to dismiss. That is, the Court found there were factual allegations that supported the plaintiff's theory of the case and that there were alternative theories as well. Relying upon its common sense and judicial experience, the Court compared a "'obvious alternative explanation'" to the theory advanced by the plaintiff and inferred that the theory advanced by the plaintiff was not a plausible conclusion. *Id.* at 682.

The Court went deeper into the analysis. It reasoned that even if the factual allegations supporting the plaintiff's theory had given rise to a plausible inference in its favor, that inference alone would not entitle it to relief. *Id.* The Court then looked deeper into the discrete nuances of the specific claims pleaded by the plaintiff to see if the complaint contained sufficient factual

allegations to support not only the claims in general, but the discrete nuances of the claims as well. *Id.* The Court found that the complaint failed to do so. The complaint failed to "'nudg[e]'" the claim "'across the line from conceivable to plausible.'" *Id.* at 683 (quoting *Twombly*, 550 U.S. at 570). Where the factual allegations fail to nudge the claim across the line from conceivable to plausible, the pleading is inadequate.

c) 3 Questions: "no" to any of these questions requires dismissal.

In summary, the Court's *Iqbal* analysis provides 3 questions to ask when analyzing a complaint to determine if it fails to state a claim:

- Ignoring all "bald allegations" and "legal conclusions," do the "factual allegations" support the elements of the claim?
- If so, does common sense and judicial experience suggest the plaintiff's theory of the claim is plausible or that there are more likely alternative explanations?
- If not, are the factual allegations supporting the discrete nuances of the claim strong enough to nudge the claim across the line from conceivable to plausible?

A "no" answer to any of these questions means the allegations in the complaint do not meet the Supreme Court's *Iqbal* standards and must be dismissed. Plaintiff's Complaint does not even make it past the first question.

2. An exemplary case demonstrates the Complaint is too vague and conclusory to state a claim—it is a mere fishing expedition for liability.

The Complaint in this case is much like the Complaint for violations of the Federal and State Wiretap Acts in *Smith v. Trusted Universal Standards In Elec. Transactions, Inc.*, 2010 WL 1799456 (D.N.J. May 4, 2010) in which the court granted a Motion to Dismiss because the Complaint at issue made only vague, conclusory and generic allegations of harm against all defendants and could only speculate as to the actual facts:

> [I]t seems clear that under *Iqbal*, Plaintiff has failed to state a claim. The Complaint merely states in a conclusory fashion that Comcast violated the Wiretap Law "by monitoring Plaintiff's Internet communications and/or allowing third parties to do so." Compl. at ¶ 65. It contains the same conclusory allegation as to

> Cisco. Compl. at ¶ 89. Plaintiff has not made any factual averments that any of his communications were in fact intercepted. If any doubt remains on that point, Plaintiff puts it to rest with his brief wherein he admits that the Complaint is a mere fishing expedition for liability:
>
> > Plaintiff does not know the exact reason for being blocked. It may be due to eavesdropping or some other reason. It is also possible that all reports, blocking and blacklisting are erroneous and *no eavesdropping took place.* Discovery is necessary to
>
> determine the exact circumstances of what happened and what devices were used, if any. Compl. at 11, ¶ 23 (emphasis added). What Plaintiff has alleged in effect is the mere possibility of liability, but not plausible liability. *See Iqbal,* 129 S.Ct. at 1949. Absent facts to support his speculation, he is not entitled to discovery to see what he may find. *See id.* at 1950 ("Rule 8 marks a notable and generous departure from the hyper-technical, code-pleading regime of a prior era, but it does not unlock the doors of discovery for a plaintiff armed with nothing more than conclusions."). On the basis of the Complaint as it now exists, Plaintiff is not entitled to relief and Comcast's and Cisco's Motions must be granted as to the Federal Wiretap Act claims.

Id. at *11.

The *Smith Court's* description of the complaint in that case accurately describes the Complaint in this case. These are the most specific allegations the Complaint offers: "Jon illegally hacked into Kate's email account, and her phone, and bank accounts." Compl. p. 1. "Jon began accessing Kate's password protected email account without her authorization." Compl. ¶ 12. "Jon also began accessing Kate's online banking accounts without her authorization, ..." Compl. ¶14. "Jon also accessed Kate's cellphone without her authorization." Compl. ¶ 15. "On information and belief, Jon has continued to access Kate's email account, online banking account, and cellphone." Compl. ¶ 23. "On information and belief, Jon's unauthorized access to known password protected accounts through the Internet has been continuous and systematic." Compl. ¶ 24. "In reality, Hoffman, Jon Gosselin, and Does 1-20, hacking in concert and on one

another's behalf, hacked into Kate Gosselin's various accounts and disseminated the illegally obtained information." Compl. ¶ 31.

As in *Smith*, the Complaint offers only conclusory allegations and has not made any factual averments that any specific computers or communications were accessed or intercepted, *see id.* at *11, which are vital allegations for the claims pleaded in the Complaint. This is exacerbated frequent "information and belief" allegations demonstrating Plaintiff is speculating.

Perhaps most telling of all, however, is the allegation "Hoffman falsely claimed in certain publications that he recovered the data from Kate's computer by digging through her trash that he found on the street. . . . The materials in his possession ***could not possibly be*** physically found in paper format to that extent. ***If*** *Hoffman was* picking through trash on the street, he did not find this trove of personal information while engaging in his trash-picking endeavors." Compl. ¶ 30. This is not a factual allegation. This is rationalization. This is conjecture. This is speculation—as to *why it had to be hacking*—because how else could it have happened, right? Or, is there a more plausible alternative explanation?

"Plaintiff has alleged in effect is the mere possibility of liability, but not plausible liability strong enough to nudge the claim across the line from conceivable to plausible. Absent facts to support [her] speculation, [s]he is not entitled to discovery to see what [s]he may find. Plaintiff is not entitled to relief" and Defendant's Motion should be granted. *Smith v. Trusted Universal Standards In Elec. Transactions, Inc.*, 2010 WL 1799456, at *11 (D.N.J. May 4, 2010). Plaintiff's claims are pure speculation, a fishing expedition, and should be treated as such.

3. A complaint premised upon allegations made upon information and belief, without real factual support, will not survive a motion to dismiss.

Allegations made upon information and belief, without factual support, do not allow the court "to draw the reasonable inference that the defendant is liable for the misconduct alleged," *Sinaltrainal v. Coca-Cola Co.*, 578 F.3d 1252, 1268 (11th Cir. 2009), and thus do not show that

the pleader is entitled to relief. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Such a complaint does not state a plausible claim for relief that will survive a motion to dismiss. *Id.*; *Wright v. Lehigh Valley Hosp. & Health Network, Inc.*, 2011 WL 2550361, at *3 (E.D. Pa. June 23, 2011).

In limited situations where the facts required to be pleaded are uniquely within the control of the defendant and not capable of being pleaded by the plaintiff, courts have made an exception and held pleading upon information and belief to be appropriate under the Twombly/Iqbal regime. *Klein v. County of Bucks*, 2013 WL 1310877 (E.D. Pa. Apr. 1, 2013). Even in these situations, the plaintiff must still plead "a proper factual basis asserted to support the beliefs pled." *Wright v. Lehigh Valley Hosp. & Health Network, Inc.*, 2011 WL 2550361, at *3 (E.D. Pa. June 23, 2011). But, where the "averments are merely 'a formulaic recitation of the elements of a cause of action' … [r]eliance by [Plaintiff] on information and belief cannot transform legal conclusions into plausible factual allegations." *Id*.

This is not a case where the facts required to be pleaded are uniquely within the control of the defendant and not capable of being pleaded by the plaintiff. All of the purported information underlying plaintiff's suspicions have been within Plaintiff's control—most likely in her own trash. The exception by which information and belief allegations may survive a motion to dismiss is inapplicable. The information and belief allegations should be ignored.

B. Seven of Plaintiff's Eight Claims are Time-Barred and Must Be Dismissed.

All but one of Plaintiff's claims have either a one or two year limitations period and are time-barred.[1] The lawsuit was filed on August 26, 2013. Plaintiff was aware of and publicly

[1] The law of this Circuit permits a statute of limitations defense to be raised by a motion to dismiss under Rule 12(b)(6), if it is obvious from the face of the complaint that the cause of action has not been timely asserted. *See Kelly v. Eckerd Corp.*, 2004 U.S. Dist. Lexis 4381, *8 (E.D. Pa. Mar. 11, 2004); *First Am. Mktg. Corp. v. Canella*, 2004 WL 25037, *5 (E.D. Pa. Jan. 26, 2004) (quoting *Robinson v. Johnson*, 313 F.3d 128, 135 (3rd Cir. 2002)); *Demetrius v. Marsh*, 560 F. Supp. 1157, 1159 (E.D. Pa. 1983).

commented on the allegations in this lawsuit roughly four years ago—at least as early as 2009.

The Complaint states "[i]n 2009, the couple separated in a high profile and public divorce. Around the same time, Jon began accessing Kate's password protected email account without her authorization." Compl. ¶¶ 11-12. The public record is replete with Plaintiff's and Plaintiff's attorneys' statements regarding these allegations claimed in this lawsuit dating back to at least 2009:

> "Kate Gosselin has heard the allegations made by Stephanie Santoro that Jon Gosselin 'hacked' into her e-mails, phone, and online accounts, and she is profoundly disturbed by them," her law firm, Schnader Harrison Segal & Lewis, said in a statement Thursday. "Under the circumstances, Ms. Gosselin is carefully considering all of her legal options regarding this matter, and she will pursue them if and when the time is right." [2]

The foregoing statement by Plaintiff's then-attorney is on a website dated October 15, 2009.[3]

1. The Federal law claims are time-barred.

The statute of limitations for each of Plaintiff's Federal law claims is two years. *See Computer Fraud and Abuse Act*, 18 U.S.C. § 1030(g); *Wiretap Act*, 18 U.S.C. § 2520(e); *Stored Communications Act*, 18 U.S.C. § 2707(f).

2. The State law claims are time-barred.

Plaintiff asserts state law tort claims against the Defendants for *Pennsylvania Wiretapping and Electronic Surveillance Act* (Count IV), *Civil Conspiracy* (Count VI), *Concerted Tortious Action* (Count VII), and *Invasion of Privacy* (Count VIII). Under Pennsylvania law, the statute of limitations for each of these tort claims is two years. *See* 42 Pa.

---

[2] New York Daily News: "Jon Gosselin sued by TLC for breach of contract; Kate may take legal action against 'hacking' claims" http://www.nydailynews.com/gossip/2009/10/16/2009-10-16_jon_gosselin_sued_by_tlc_for_breach_of_contract_kate_may_take_legal_action_again.html

[3] Kate Gosselin Considering Legal Options Against Jon After Reading Radar Report, http://radaronline.com/exclusives/2009/10/kate-gosselin-considering-legal-options-against-jon-after-reading-radar-report/

C.S.A. § 5524; *Stauffer v. Bell Atl.*, 2002 WL 32349886 (E.D. Pa. Feb. 20, 2002) *aff'd*, 85 Fed. Appx. 874 (3d Cir. 2003) ("A civil cause of action for violation of Pennsylvania's wiretapping law, 18 Pa.C.S.A. § 5725, is governed by the two-year statute of limitations for actions founded on negligent, intentional, or otherwise tortious conduct."); *Shivone v. Washington Mut. Bank, F.A.*, 2008 U.S. Dist. LEXIS 59212, at *8 (E.D. Pa. Aug. 5, 2008) (conspiracy and aiding and abetting claims subject to two year limitation period set forth in 42 Pa. C.S.A. § 5524); *Brock v. Thomas*, 782 F. Supp. 2d 133, 140-41 (E.D. Pa. 2011) ("[C]laims of . . . civil conspiracy, and concerted tortious conduct . . . . have a two-year limitations period that begins to run on the date of injury."); 42 Pa. Cons. Stat. Ann. § 5523 (West) ("The following actions and proceedings must be commenced within one year . . . An action for libel, slander or invasion of privacy.").

3. The Court may take judicial notice of Plaintiff's awareness in 2009 of the allegations—it is publicly available information that is both generally known and capable of accurate and ready determination.

A basic Google search produces numerous results for Plaintiff's statement by her attorney in 2009 stating her awareness of the allegations now made in this lawsuit and how, at the time, she was "carefully considering all of her legal options regarding this matter, and she [would] pursue them if and when the time is right."[4] This event is not only common knowledge, but is undeniable by Plaintiff.

Precedent in this district demonstrates that the Court can properly take judicial notice of information such as these websites where the matter is in the public domain and is both generally known and capable of accurate and ready determination. *See Wilson v. City of Philadelphia*, 2010 WL 1254111 (E.D. Pa. Mar. 31, 2010), *vacated in part on other grounds*, 415 Fed. Appx.

[4] New York Daily News: "Jon Gosselin sued by TLC for breach of contract; Kate may take legal action against 'hacking' claims" http://www.nydailynews.com/gossip/2009/10/16/2009-10-16_jon_gosselin_sued_by_tlc_for_breach_of_contract_kate_may_take_legal_action_again.html

434 (3d Cir. 2011). The *Wilson* Court was considering a motion to dismiss premised on official immunity issues that required facts concerning the dates and roles of defendant's prior employment. This information was not available in the complaint or any incorporated documents. In granting the motion to dismiss, the court took judicial notice of information from the defendant's biography page on a law firm's website. *Wilson*, 2010 WL 1254111, at n.4.

Similarly, in *Inman v. Technicolor USA, Inc.*, 2011 WL 5829024 (W.D. Pa. Nov. 18, 2011), the court was considering a motion to dismiss concerning the interpretation of a website User Agreement that was neither attached to the complaint nor specifically referenced therein but the court determined that it was proper to take judicial notice of the website in granting the motion to dismiss. *Inman*, 2011 WL 5829024, at 3-4.

4. The information properly before the Court shows that in 2009, Plaintiff was aware of the allegations upon which this suit is premised and all but one of her claims are time-barred by limitations.

The timeline of the case is straightforward. In 2009, Plaintiff was aware of allegations that "Jon Gosselin 'hacked' into her e-mails, phone, and online accounts," she was profoundly disturbed by them, and she was "carefully considering all of her legal options regarding this matter, and she [would] pursue them if and when the time is right."[5] Now, roughly four years later, Plaintiff has apparently determined that the time is right. Indeed, the Complaint was filed one month prior to the release of her new cookbook. However, all of Plaintiff's claims, except for the Identity Theft claim, are governed by a statute of limitations of two years or less and are time-barred. These seven claims should be dismissed with prejudice.

---

[5] New York Daily News: "Jon Gosselin sued by TLC for breach of contract; Kate may take legal action against 'hacking' claims" http://www.nydailynews.com/gossip/2009/10/16/2009-10-16_jon_gosselin_sued_by_tlc_for_breach_of_contract_kate_may_take_legal_action_again.html

C. Plaintiff Failed to Adequately Plead Virtually Every Required Element of the CFAA Claim (Count I).

In Count 1 of the Complaint, Plaintiff seeks to invoke the civil remedy of the Computer Fraud and Abuse Act (CFAA) by asserting a claim pursuant to 18 U.S.C. § 1030(a)(2)(c). Compl. ¶ 40. The elements of a civil claim for a violation of section 1030(a)(2) require the plaintiff to show that the defendant did the following: (1) intentionally accessed a protected computer, (2) without authorization or exceeding authorized access, and that he (3) thereby obtained information (4) from any protected computer, and that (5) there was a loss to one or more persons during any one-year period aggregating at least $5,000 in value.

Plaintiff failed to adequately plead and identify the computers that were allegedly accessed, that such specific computers were protected computers, and that there was jurisdictionally threshold loss.

1. The Court does not have jurisdiction to consider the CFAA claim because Plaintiff does not meet the $5,000 loss threshold requirement.

In order to bring a civil claim under the CFAA, Plaintiff must plead that, during any one-year period, she sustained a loss of at least $5,000 because of the CFAA violation. *A.V. ex rel Vanderhyne v. iParadigms, LLC*, 562 F.3d 630, 646 (4th Cir. 2009). This requirement is essential to meeting the jurisdictional threshold for a court to hear the claim, and was purposely implemented by Congress to keep from clogging the courts with trivial cases by "limit[ing] federal jurisdiction to cases of substantial computer crimes." *In re Doubleclick, Inc. Privacy Litig.*, 154 F. Supp.2d 497, 522 (S.D.N.Y. 2001). This *loss* requirement is a jurisdictional threshold that must first be satisfied before the court is vested with jurisdiction to decide the case even if the *damages* are in the millions. *See Quantlab Techs. Ltd. (BVI) v. Godlevsky*, 719 F. Supp.2d 766, 776 (S.D. Tex. 2010).

The terms *loss*, *damage*, and *damages* each have their own unique meaning under the CFAA. They are not interchangeable. *See* 18 U.S.C. § 1030(g). Because a civil action is only available if the violation involves at least one of five subsection (c)(4)(A)(i) factors, the requirements of that subsection must be satisfied or the civil remedy is not available.

It appears as though Plaintiff is attempting to invoke sub-clause (I) but the allegation misses the mark: "Defendants accessed Kate Gosselin's computer and computer services without authority to do so and in doing so, caused in excess of $5,000 worth of damage." Compl. ¶ 47. This conclusory statement as to alleged damage is inadequate.

Sub-clause (I) does not include damage; only "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." The term loss is defined by the CFAA:

> [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). Plaintiff does not allege there was an interruption of service and, in all other cases, a loss generally means a cost, *Sealord Holdings, Inc. v. Radler*, 2012 WL 707075 (E.D. Pa. Mar. 6, 2012), which Plaintiff has not alleged. "Claims of lost business opportunities, damaged reputation, loss of assets, and other missed revenue, however, do not constitute 'loss.'" *Sealord Holdings, Inc. v. Radler*, 2012 WL 707075 (E.D. Pa. Mar. 6, 2012). The Third Circuit cases are clear on what constitutes a "loss," which is not pleaded here. "A compensable 'loss' under the CFAA ... is the cost of remedial measures taken to investigate or repair the damage to the computer, or the loss is the amount of lost revenue resulting from a plaintiff's inability to utilize the computer while it was inoperable because of a defendant's misfeasance." *Brooks v. AM Resorts, LLC*, 2013 WL 3343993, at *5 (E.D. Pa. July 3, 2013) (quoting *Clinton Plumbing & Heating of Trenton, Inc. v. Ciaccio*, 2011 WL 6088611, at *5 (E.D. Pa. Dec.7, 2011). Plaintiff

has failed to plead the requisite loss necessary to invoke the Court's jurisdiction to entertain a civil claim under the CFAA. The motion to dismiss this claim should be granted.

2. The Complaint fails to allege any specific wrongful accesses to any identifiable "protected computer."

The CFAA is an access violation. "The CFAA expressly prohibits improper 'access' of computer information. It does not prohibit misuse or misappropriation." *United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012). "[T]he word 'access,' in this context, is an active verb: it means 'to gain access to,' or 'to exercise the freedom or ability to make use of something.'" *Role Models Am., Inc. v. Jones*, 305 F. Supp.2d 564, 567 (D. Md. 2004) (quoting *Am. Online, Inc. v. Nat'l Health Care Discount, Inc.*, 121 F. Supp.2d 1255, 1272–73 (N.D. Iowa 2000)). The receipt of information that has come from a computer is not an access of that computer and not prohibited by the CFAA. *Id.* at 566-67. Because the CFAA governs activity that involves accessing or damaging computers, the access to and use of the computer is integral to the CFAA and not merely incidental. *Dresser-Rand Co. v. Jones*, 2013 WL 3810859, *4 (E.D. Penn. July 23, 2013). "Whatever happens to the data subsequent to being taken from the computer subsequently is not encompassed in the purview of the CFAA." *Id.* The most important allegation for a CFAA violation is the access of a computer. *See id.* The issue of access is one of the most confusing, uncertain, and frequently litigated issues under the CFAA.

"[T]he Third Circuit has explained that the factual allegations in the complaint may not be 'so undeveloped that it does not provide a defendant the type of notice which is contemplated by Rule 8.' *Phillips v. County of Allegheny*, 515 F.3d 224, 233 (3rd Cir. 2008). Moreover, 'it is no longer sufficient to allege mere elements of a cause of action; instead "a complaint must allege facts suggestive of [the proscribed] conduct."' *Id.* (alteration in original) (quoting *Twombly*, 550 U.S. at 563 n. 8)." *Sealord Holdings, Inc. v. Radler*, 2012 WL 707075 (E.D. Pa. Mar. 6, 2012).

The sole allegations touching upon "access" in the Complaint are these conclusory statements:[6]

> Jon illegally hacked into Kate's e-mail account, and her phone, and bank accounts. Compl. p.1.
>
> Around the same time [2009], Jon began accessing Kate's password-protected e-mail account without her authorization. Compl. ¶ 12.
>
> Jon also began accessing Kate's online banking accounts without her authorization,…. Compl. ¶ 14.
>
> Jon also accessed Kate's cellphone without her authorization. Compl. ¶ 15.

a) The email and bank accounts are not identifiable computers.

An e-mail account and bank account, in and of themselves, are not computers under the CFAA. The CFAA defines "computer" as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device." 18 U.S.C. § 1030(e)(1). "Under the CFAA, a 'protected computer' is one '[w]hich is used in interstate or foreign commerce or communication.' 18 U.S.C. § 1030(e)(2)(B). Such devices include 'any data storage facility or communications facility directly related to or operating in conjunction with' a computing system. *Id.* § 1030(e)(1)." *Integrated Waste Solutions, Inc. v. Goverdhanam*, 2010 WL 4910176 (E.D. Pa. Nov. 30, 2010).

Cellphones are considered computers under this definition. *United States v. Kramer*, 631 F.3d 900, 901 (8th Cir. 2011). Identified websites are also considered to be computers because

---

[6] The Complaint fails to make even a single allegation of access of any computer as to any of the Defendants, including Defendants Robert Hoffman and John and Jane Does 1-20. *See* Compl.

accessing a website necessarily requires accessing the server hosting the site, which is a computer. *LVRC Holdings, LLC v. Brekka*, 581 F.3d 1127, 1136 (9th Cir. 2009).

The Complaint only makes a conclusory allegation of accessing an "email account" and "bank account" or "online bank account" without any further information, most of which is made on information and belief, which is of no value for this motion to dismiss. *See* Section I.D.2, *supra*. It is impossible to know whether those accounts of the information therefrom was stored or backed up locally on a computer for which Defendant was authorized to access, whether there was simply data from those accounts that was stored on removable storage devices, whether their information was aggregated into one cloud-based service such as Dropbox or Google Drive, or whether Plaintiff is claiming Defendant logged into specific websites that hosted certain email or banking applications. For example, had the information from the email or bank accounts been backed up and stored on Defendant's own computer, there would be no violation of the CFAA under the precedent of *Dresser-Rand Co. v. Jones*, 2013 WL 3810859, *4 (E.D. Penn. July 23, 2013) ("Wadsworth may have accessed Dresser-Rand documents, but he never accessed Dresser-Rand computers, as required under the CFAA.").

One thing that is clear, however, is that neither an amorphous "email account" or "online bank account" satisfy the definition of computer set forth in 18 U.S.C. § 1030(e)(1); the claim regarding the email account and bank account do not allege an access to a computer or how and when they were allegedly accessed and should be dismissed.

"[C]ourts in the Eastern District of Pennsylvania have generally adopted the narrow interpretation" in which one who is given access to a computer is authorized to access the computer regardless of his or her intent to miss use information. *Dresser-Rand Co. v. Jones*, 2013 WL 3810859, *4 (E.D. I3810859, *4 (E.D. Penn. July 23, 2013). Accordingly, to determine whether an access to a computer "exceeds authorized access" or is "without authorization", it is

imperative to know the identity of the specific computer allegedly accessed, when it occurred, and how it occurred to determine what rights (if any) the person had to access the computer in general. The Complaint does not identify any specific computer associated with the alleged access of e-mail or online banking accounts.

b) The Complaint does not allege how or when the cellphone was allegedly accessed.

The Complaint is completely devoid of allegations on how Defendant allegedly accessed Plaintiff's cellphone. The Complaint does not allege any interaction with any identifiable computers, computer systems, or network other than the cellphone, however, it does not allege when or how the access was to have occurred. This information is especially important in a situation such as this where the Plaintiff and Defendant had been married and, presumably, had authorization to access the computers within their home. Under the narrow interpretation, if those rights have access had changed, there must be some basis for analyzing when and how that authorization changed as well as what objectively verifiable notice of the change was provided.

3. The CFAA does not permit recovery of punitive damages, costs or legal fees.

The only damages Plaintiff could be entitled to under the CFAA are economic damages. 18 U.S.C. 1030(g). The CFAA does not permit the recovery of punitive damages, *see Liebert Corp. v. Mazur*, 2004 WL 2095666, at *3 (N.D. Ill. Sept. 17, 2004), or litigation costs and attorneys' fees incurred for the prosecution or defense of a CFAA claim, *see Thundervision, LLC v. Dror Int'l, LP*, 2010 WL 2219352, at *12 (Bankr. E.D. La. June 1, 2010).

D. The Complaint Fails To Adequately Plead Several Requirements Of The ECPA "Wiretap Act" Claim (Count II) And Pennsylvania Wiretapping And Electronic Surveillance Act Claim (Count IV).

1. The Pennsylvania Wiretapping and Electronic Surveillance Act is interpreted identical to The Federal Wiretap Act.

In this section Defendant simultaneously addresses both the Federal Wiretap Act and the

Pennsylvania Wiretapping and Electronic Surveillance Act. The Complaint makes the same allegations for both claims and they are interpreted identically. "The Pennsylvania act tracks the language set forth in the Federal Act, and has been interpreted identically." *Ideal Aerosmith, Inc. v. Acutronic USA, Inc.*, CIV.A. 07-1029, 2007 WL 4394447 (E.D. Pa. Dec. 13, 2007).

2. No allegation of an interception of any contents of a communication.

The Wiretap Act defines "intercept" as "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). As explained in Section IV.A.3., *supra*, the Complaint "has not made any factual averments that any of [her] communications were in fact intercepted." *Smith v. Trusted Universal Standards In Elec. Transactions, Inc.*, 2010 WL 1799456, at *11 (D.N.J. May 4, 2010). There are no allegations that any communications were intercepted, much less the contents of communications, which is what is mandatory. 18 U.S.C. § 2510(8).

Plaintiff fails to identify specific communications that she sent that were intercepted. This is required to state a claim under the Wiretap Act because "Plaintiff has standing to assert claims only with respect to those communications sent by Plaintiff . . ., not with respect to those communications sent by third parties." *Ideal Aerosmith, Inc. v. Acutronic USA, Inc.*, 2007 WL 4394447, *4 (E.D. Pa. Dec. 13, 2007).

3. No allegation of interception of a communication contemporaneous with transmission.

Under the ECPA "an 'interception' of an e-mail must 'occur contemporaneously with the transmission.'" *Reichert v. Elizabethtown Coll.*, 2011 WL 3438318, *4 (E.D. Pa. Aug. 5, 2011) (quoting *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113 (3d Cir. 2003)). If the communication is not intercepted simultaneously, it is not a violation of the Wiretap Act. Communications that had been sent or received are not prohibited by the Wiretap Act. Plaintiff fails to identify any such alleged communications.

4. No allegation of any device—specific hardware or software—that was purportedly used.

"[I]n order to state a claim under the Wiretap Act, a plaintiff must allege that a communication was intentionally intercepted through the use of a device." *Ideal Aerosmith, Inc. v. Acutronic USA, Inc.*, 2007 WL 4394447, at *4 (E.D. Pa. Dec. 13, 2007). The Complaint fails to allege that any particular device was used to intercept a communication, much less a device used for each of the unique classes of communications such as email, bank account, and cell telephone.

E. The Complaint Fails To Adequately Plead Requirements Of The SCA (Count III).

The Stored Communications Act "creates civil liability for one who '(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system.'" *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114 (3d Cir. 2003).

1. Complaint fails to allege a facility for each of the classes of communications claimed: email, bank account, and cellphone.

The Complaint fails to allege that Defendant accessed a specific facility through which an electronic communication service was provided. An electronic communication service is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Plaintiff has failed to allege a specific facility for each category of communications underlying its claim: email, bank account, cellphone.

2. Complaint fails to allege the location or timing of the communications.

The Complaint fails to identify the location of the particular communications at the time of the alleged access, which is relevant to determining whether Plaintiff has stated a claim. *See*

Brooks v. AM Resorts, LLC, 2013 WL 3343993, *4 (E.D. Pa. July 3, 2013) ("The parties agree that email messages remaining on an internet service provider's server after delivery fall within the Act's definition of electronic storage. . . . Moreover, no one contests that emails downloaded and stored on a personal computer are not included in the Act's definition of electronic storage."). Unless, at the time of the access, the communications were in "electronic storage of the electronic communications service itself," *Thompson v. Ross*, 2010 WL 3896533, at *3-4 (W.D. Pa. Sept. 30, 2010), there is no violation of the SCA. A communication subject to the SCA must have been accessed while it was in "electronic storage" which has a narrow, statutorily defined meaning: "[E]lectronic storage" is "(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. § 2510(17).

To state a claim for violation of the SCA, the Complaint must allege facts indicating that each particular communication allegedly wrongfully accessed was in "electronic storage," which it has failed to do. Specificity as to whether the communication had been received by Plaintiff's service provider but had not yet been accessed by Plaintiff, or had been accessed and was retained by Plaintiff, is necessary to make this determination. If the Plaintiff chose to retain a copy of the communication on the service provider's system, the retained copy was no longer in "electronic storage" because it was no longer in "temporary, intermediate storage … incidental to … electronic transmission," and neither is it a backup of such a communication. *See Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp.2d 623, 635-36 (E.D. Pa. 2001), *aff'd in part* 352 F.3d 107, 114 (3rd Cir. 2004). The Complaint completely fails to address this issue as to each category of communications, much less each particular communication allegedly wrongfully accessed.

F. The Complaint Fails To Adequately Plead Several Requirements Of The Identity Theft Claim (Count V).

Count VI asserts a claim of "identity theft" against Defendant pursuant to 42 Pa. C.S.A. § 8315, which allows an individual to asset a civil claim of identity theft in connection with a violation of 18 Pa. C.S.A. § 4120(a): "[a] person commits the offense of identity theft of another person if he possesses or uses, through any means, identifying information of another person without the consent of that other person to further any unlawful purpose."

1. Complaint fails to allege any qualifying identifying information.

The Complaint fails to allege what, if any, "identifying information" was allegedly possessed or used by Defendant. A careful reading of the statutory definition of the term "identifying information" is critical to properly evaluating this claim because a violation of the statue can only come through using "identifying information," as defined:

> "Identifying information." Any document, photographic, pictorial or computer image of another person, or any fact used to establish identity, including, but not limited to, a name, birth date, Social Security number, driver's license number, nondriver governmental identification number, telephone number, checking account number, savings account number, student identification number, employee or payroll number or electronic signature.

18 Pa. Cons. Stat. Ann. § 4120 (West). The plain reading of the statute indicates that there can be only two categories of "identifying information:" (1) an image of another person (which can be either a document, photographic, pictorial, or computer image); or (2) a fact used to establish identity. The Complaint does not identify what particular information Plaintiff alleges Defendant possessed and used to further any unlawful purpose.

2. Publicly available information about Plaintiff cannot be "identifying information" under the statute.

Plaintiff's case does raise a unique situation, however, because, as she pleads her "celebrity status," Compl. ¶ 19, she raises an important issue: information that is publicly

available is not unlawfully possessed for purposes of the Identity Theft statute. *See Eagle v. Morgan*, 2013 WL 943350, at *9 (E.D. Pa. Mar. 12, 2013).

3. The Identity Theft statute is limited to situations where "identifying information" is being used to impersonate an identity—not write a book.

A plain reading of the law indicates that it is designed to prohibit one person from misusing identifying information of another persona for purposes of establishing identity for unlawful purposes. *See* 18 Pa. C.S.A. § 4120(a). That is the purpose stated by the State of Pennsylvania on its *Identity Theft Action Plan* website[7] answering "What is Identity Theft?"

> Identity theft is a serious crime that occurs when someone else uses your personal information such as your name, Social Security Number, credit card information, driver's license number or other identifying information without your permission.
>
> Most of the time, this stolen information is used to obtain credit, merchandise or services in the name of the victim. But, in addition to running up debt, an imposter might provide false identification to police, creating a criminal record or leaving outstanding arrest warrants for the person whose identity has been stolen.

This is consistent with the statutory remedies available for violation of the Identity Theft statute. *Restitution for Identity Theft*, 18 Pa. C.S.A. § 1107.1 provides for restitution "(1) to investigate theft of the victim's identity; (2) bring or defend civil or criminal actions related to theft of the victim's identity; or (3) to take other efforts to correct the victim's credit record or negative credit reports related to theft of the victim's identity." *Id.*

4. Complaint fails to establish so clearly an unlawful purpose that it constitutes identity theft.

To constitute identity theft, the purpose for which "identifying information" is used must be a clearly unlawful purpose. *Eagle v. Morgan*, CIV.A. 11-4303, 2013 WL 943350, at *9 (E.D. Pa. Mar. 12, 2013). The Complaint alleges that disclosing the information allegedly gained

through alleged violations of the CFAA, ECPA, SCA, and PWESA, "and then disclosing their contents to a book publisher, and using this highly-sensitive and unlawfully obtained information to publish an untrue book defaming Kate," Defendant violated the Identity Theft statute. Compl. ¶ 84. The Complaint does not allege that the "identifying information" was used to further such a clearly unlawful purpose as to establish identity for illegally obtaining goods and services, which is what is customary under the Identity Theft Statute.

G. The Complaint Fails To Adequately Plead Several Requirements Of The Civil Conspiracy Claim (Count VI) and Concerted Tortious Action Claim (Count VII).

Under Pennsylvania law, to sufficiently plead an action for civil conspiracy or concerted tortious conduct, a complaint must sufficiently allege an existing independent wrong or tort that would constitute a valid cause of action. Unless there is a finding that the underlying tort has occurred, there can be no claim for civil conspiracy, *Eagle v. Morgan*, 2013 WL 943350, at *11 (E.D. Pa. Mar. 12, 2013), or concerted tortious action, *State Farm Mut. Auto. Ins. Co. v. Ficchi*, 2011 WL 2313203, at *13 (E.D. Pa. June 13, 2011). As discussed above, the Complaint does not adequately plead an independent wrong or tort that will support a claim for conspiracy or concerted tortious action. Counts VI and VII should be dismissed.

Under Pennsylvania law, an essential element of a conspiracy claim is the proof of malice which "[r]equires that the sole purpose of the conspiracy was to injure the plaintiff and that this intent to injure be without justification." *Eagle v. Morgan*, 2013 WL 943350, at *11 (E.D. Pa. Mar. 12, 2013). This element is conclusively negated where the Complaint shows another purpose for the alleged activities. *Id.* The Complaint affirmatively alleges that Defendant Robert Hoffman is a reporter, Compl. ¶ 25, that the information allegedly giving rise to these claims was

---

[7] What is Identity Theft (visited Sept. 17, 2013)
http://www.portal.state.pa.us/portal/server.pt/community/what_is_id_theft_/12993/what_is_identity_theft_/584645

published in several publications, Compl. ¶ 28, that Defendants Hoffman and Gosselin were paid for this information by various publications, Compl. ¶ 32, which payments escalated, Compl. ¶ 33, and finally the information was used by Defendant Hoffman to publish a book, Compl. ¶ 34, and finally and most importantly, alleges that the Defendants did these things "for the purpose of profiting from the book and the tabloid publications, Compl. ¶ 37. Plaintiff's own pleading affirmatively negates her conspiracy claim.

H. The Complaint Fails To Adequately Plead Several Requirements Of The Invasion Of Privacy Claim (Count VIII).

The Complaint is deficient in that it fails to even allege the particular basis of the Invasion of Privacy claim in Count VIII. "Under Pennsylvania law, invasion of privacy encompasses four separate torts: (1) unreasonable intrusion upon the seclusion of another; (2) appropriation of another's name or likeness; (3) publicity given to another's private life; and (4) publicity that unreasonably places another in a false light before the public." *Rodriguez v. Widener Univ.*, 2013 WL 3009736, at *9 (E.D. Pa. June 17, 2013). Plaintiff's failure to plead the basis for her Invasion of Privacy claim is inadequate, requiring dismissal.

The Complaint does not allege that the information claimed disclosed was not true. In the event Plaintiff's conclusory claim for Invasion of Privacy purports to assert a claim under the separate torts identified as (1), (3), or (4) above, "there can be no liability when the statement is true." *Rodriguez v. Widener Univ.*, 2013 WL 3009736, at *10 (E.D. Pa. June 17, 2013); *See Chan v. County of Lancaster*, 2013 WL 2412168, at *28 (E.D. Pa. June 4, 2013). The only categories of information Plaintiff mentions are "family photos, personal documents, tax and business records plus contracts," Compl. ¶ 26, most of which are items that Plaintiff *should* hope are not false. Any Invasion of Privacy claim premised on the above torts should be dismissed.

Respectfully submitted,

Dated: September 18, 2013

/s/ *Shawn E. Tuma*

Shawn E. Tuma (pro hac vice pending)
BrittonTuma
7161 Bishop Road, Suite 220
Plano, Texas 75024
d. 469.635.1335
f. 972.767.3181
e. stuma@brittontuma.com

Richard L. Orwig (Associate Counsel)
Orwig Law Offices
2213 Quarry Dr., Suite B001
West Lawn, PA 19609
p. 610.898.9880
f. 610.898.1323
e. rlorwig@orwiglaw.com

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true and correct copy of the foregoing document has been served upon all counsel of record in the above-styled civil action through the Court's electronic filing system on this 18th day of September, 2013.

/s/ *Shawn E. Tuma*
Shawn E. Tuma