IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

DAVID EGILMAN, Plaintiff, v. KELLER and HECKMAN LLP, et al., Defendants.	)	No. 1:04-CV-876-HHK

MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF MOTION OF DEFENDANTS KELLER AND HECKMAN LLP AND DOUGLAS J. BEHR FOR JUDGMENT ON THE PLEADINGS

Defendants Keller and Heckman LLP ("K&H") and Douglas J. Behr ("Behr") ("Defendants") submit this memorandum in support of their motion, pursuant to Rule 12(c) of the Federal Rules of Civil Procedure, for judgment on the pleadings dismissing the Verified Complaint ("Ver. Compl.") filed by plaintiff David Egilman ("Egilman").

FACTS

Egilman has sued the law firms of Jones Day and Keller and Heckman, along with K&H partner Behr, for allegedly violating two federal statutes and committing common law torts, including trespass.[1] The three counts pled by Egilman arise out of a

[1] The federal statutory claims are 18 U.S.C. § 1030, the Computer Fraud and Abuse Act ("CFAA") (Ver. Compl. ¶¶ 25-28), and 17 U.S.C. § 1201, et seq., the Digital Millennium Copyright Act ("DMCA") (*Id.* at ¶¶ 29-32). An unspecified common law claim is asserted under the laws of the District of Columbia, Massachusetts and Texas, while that of trespass to Egilman's computer is asserted under the law of no particular jurisdiction. *Id.* at ¶¶ 33-35.

2001 judicial proceeding, *Ballinger, et al. v. Brush Wellman Inc.*, No. 96-CV-2532, in the District Court for the First Judicial District, Jefferson County, Colorado (hereinafter, *Ballinger*). In *Ballinger*, Egilman – a professional expert witness for the plaintiffs in that case – was sanctioned for willfully violating a court order by publishing derogatory information about the presiding judge.

On May 30, 2001, shortly before trial, the *Ballinger* court issued a restraining order that, *inter alia*, prohibited the parties, their counsel, expert witnesses, and other witnesses under the parties' control, from publishing statements on Internet websites concerning the trial proceedings, participants, issues or evidence. *See* Ex. A, *Ballinger*, Order Prohibiting Certain Extrajudicial Statements (May 30, 2001) (the "Court's Order").* The restraining issue was ordered based on the court's reaction to materials posted by Egilman on his website. *Id.*

In response to the Court's Order, Egilman then posted to his website the assertion that the *Ballinger* trial judge had been bribed: "Colorado Judge in Jones Day Pocket: What did it cost?" and "New FORMERLY SECRET, Jones-Day dirt-criminal activity: ITS HERE FOR ALL TO SEE." *See* Ex. B, pages from *Ballinger* Def. Ex. 2000. Egilman's comments were discovered and brought to the attention of the court by Kelly Stewart, and other partners of Jones Day, which represented the lead defendant, Brush Wellman, in the *Ballinger* matter. At his deposition in the related Texas action that

---

* All references to "Ex. _" are to the exhibits attached to the accompanying Declaration of Jeffrey P. Cunard, dated August 16, 2004.

preceded this one in the District of Columbia,[2] Mr. Stewart testified that he gained access to Egilman's website by using the rudimentary and obvious (given Egilman's professional affiliation with Brown University and his apparent intent to publish the website to his students at Brown University) username/password combination of "Brown" and "student." Stewart had learned that combination from Behr, who had informed him about the scurrilous information on Egilman's website.

Egilman alleges that he maintained this website on his own personal computer. Ver. Compl. ¶ 9. The site could be accessed via the Internet by typing in www.egilman.com and, indeed, prior to the entry of the Court's Order, the website had been accessible to the general public. Egilman could have complied with the Court's Order either by removing the offending comments and material from www.egilman.com or, alternatively, shutting the website down. He did not. Instead, Egilman claims to have complied with the Order because he "restricted access" to www.egilman.com (Ver. Compl. ¶ 13) by requiring users to enter a user name and password before they could

---

2 In June 2002, Egilman commenced an action against Jones Day in Texas state court (the "Texas Action"). *See* Ex. C, Pl.'s Original Pet., *Egilman v. Jones, Day, Reavis & Pogue, et al.*, Cause No. 20140*BH02 (Dist Ct. Brazoria County, Texas). In the Texas Action, he made essentially the same claims brought as Count III in this action, that Jones Day's unauthorized access to the false entry placed on his website violated various property rights he enjoyed in his computer. Egilman amended his Original Petition in the Texas Action four times, including to add K&H and Behr as defendants. (The action was also transferred to Harris County, Texas.) *See* Ex. D, Civil Case Summary, *Egilman v. Jones, Day, Reavis & Pogue, et al.*, Cause No. 2003-25162 (Dist. Ct. Harris County, Texas.)

view its contents. Ver. Compl. ¶¶ 11, 13. According to Egilman, those who were able to have access to his website, despite the Court's Order, "were dues-paying subscribers," which "included corporations, companies, law firms (both big and small), individual lawyers and individuals." *See* Ex. E, Affidavit of David Egilman at 2, *Egilman v. Jones, Day, Reavis & Pogue, et al.*, Cause No. 2003-25162 (Dist Ct. Harris County, Texas) (Dec. 18, 2003) (filed in support of plaintiff's response to defendants' motion to compel discovery responses). (Egilman has not explained how publishing his website to "authorized" users would comply with the Court's Order.) Furthermore, Egilman concedes that he anticipated that certain "unauthorized parties" would gain access to his site. Ver. Compl. ¶ 14.

Instead, Egilman alleges that he baited a trap. According to Egilman, he placed the claim about Jones Day having bribed the Colorado judge on his website expecting it to be made public. According to the Complaint, Egilman was "concerned that unauthorized parties were attempting to access restricted content on his Website" and that he placed a "false entry" on the website so that, if the entry became public, his suspicions would be proved true. *Id.* Defendant Jones Day is alleged to have "presented the illegally obtained pages" to the Colorado trial court, with the court citing to those documents as proof that Egilman had violated its Order. Ver. Compl. ¶ 23.

As a result of that violation, the court sanctioned Egilman. *See* Ex. F, *Ballinger*, Findings, Conclusions, and Orders Concerning Sanctions (June 22, 2001) (the "Sanctions Order"). It ordered that his testimony in *Ballinger* be stricken, the jury was instructed to disregard that testimony and Egilman was prohibited from testifying in any later case in

that court. *See* Sanctions Order at 2-3. The finding that Egilman's posting had, in fact, violated the Court's Order was affirmed by the Colorado Court of Appeals.[3]

A year after the Sanctions Order, Egilman commenced the Texas Action against Jones Day for Texas common law claims arising out of the alleged illegal entry into his computer. In December 2002, Egilman made one of his four separate amendments to his petition in the Texas Action, to add K&H and Behr as having been involved in bringing the false entry to the attention of the *Ballinger* court in June 2001. *See* Ex. H, Pl.'s 2nd Am. Original Pet., *Egilman v. Jones, Day, Reavis & Pogue*.[4] He alleged that Behr provided a Jones Day partner with the username and password to his website. The Texas

---

[3] The prospective sanction that prohibited Egilman from testifying in the future, however, was vacated on the grounds that Egilman should have been given an opportunity to participate in the sanctions proceeding. *See* Ex. G, Orders Affirmed in Part, and Vacated in Part, *Egilman v. District Court, et al.*, No. 01CA1982 (Colo. Ct. App. Sept. 5, 2002).

[4] This Court may take judicial notice of this and the other filings made in the Texas Action under FED. R. EVID. 201(b) (a court may take judicial notice of adjudicative facts that are "capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned"). These documents are included not for the facts asserted, but to show the nature of Egilman's prior claims. *See Petrick v. Am. Mgmt. Sys.*, No. 01-7197, 2003 U.S. App. LEXIS 3720 (D.C. Cir. 2003) ("a court may take judicial notice of a document filed in another court not for the truth of the matters asserted in the other litigation, but rather to establish the fact of such litigation and related filings") (citing *Liberty Mut. Ins. Co. v. Rotches Pork Packers, Inc.*, 969 F.2d 1384, 1388-89 (2d Cir. 1992)). Although Egilman's responses to discovery requests are not documents filed with the courts, that he took the positions expressed therein cannot be reasonably questioned. *See, e.g., United Dairy Farmers, Inc. v. United States*, 267 F.3d 510, 512 (6th Cir. 2001) (where court granted motion to take judicial notice of certain discovery responses); *Insurance Co. of N. Am. v. Hilton Hotels U.S.A.*, 908 F. Supp. 809, 813 (D. Nev. 1995), *aff'd*, 110 F.3d 715 (9th Cir. 1997) (same).

Action, however, never was resolved on the merits. On March 10, 2004, with the possibility of sanctions for multiple failures to comply with discovery and facing his own deposition, Egilman voluntarily dismissed his claims. *See* Ex. I, Notice of Non-Suit Without Prejudice As to All Defendants, *Egilman v. Jones, Day, Reavis & Pogue, et al.*; Ex. D, Civil Case Summary (setting forth discovery motions and orders).

This federal proceeding is, therefore, nothing more than a recycling of the same facts in the guise of alleged violations of the CFAA and the DMCA, and a reassertion of Egilman's Texas Action property rights claim in Count III.

ARGUMENT

Judgment on the pleadings should be entered against a plaintiff when the allegations of the complaint, even if assumed true, fail to state a claim upon which relief may be granted. In evaluating the allegations in the pleading, the Court may consider matters incorporated into the pleadings by reference and matters of which judicial notice may be taken. *Chandamuri v. Georgetown Univ.*, 274 F. Supp. 2d 71, 77 (D.D.C. 2003) (in context of Rule 12(b)(6) motion, citing *EEOC v. St. Francis Xavier Parochial Sch.*, 117 F.3d 621, 624-25 (D.C. Cir.1997)); *Does I v. D.C.*, 238 F. Supp. 2d 212, 216 (D.D.C. 2002) ("courts 'are allowed to take judicial notice of matters in the general public record, including records and reports of administrative bodies and records of prior litigation'" in a 12(c) motion without converting the motion to one for summary judgment (quoting *Black v. Arthur*, 18 F. Supp. 2d 1127, 1131 (D. Or. 1998), *aff'd on other grounds*, 201 F.3d 1120 (9th Cir. 2000)).

Egilman's allegations are unusually vague and conclusory. Accordingly, this Court may, and should, review his more detailed allegations and responses to discovery requests from the overlapping Texas Action he dismissed just this past March. Even when accepting all of those details as true, however, dismissal under Rule 12(c) remains appropriate.[5]

I. The CFAA Claim Is Time Barred And Defective On The Merits.

In Count I, Egilman purports to state a claim under the Computer Fraud and Abuse Act ("CFAA"). The CFAA, the principal federal statute outlawing computer hacking, originally was enacted in 1984. It has been broadened several times since, including, most recently, in October 2001, as part of the USA PATRIOT Act.[6]

A. The Statute of Limitations Has Run On Egilman's CFAA Claim.

The CFAA provides that

> no action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage.

18 U.S.C. § 1030(g). The plain language of that provision means that the statute of limitations ran on any CFAA claim Egilman might try to assert over a year ago, in June 2003.

---

[5] Pleadings and discovery responses are within the scope of judicial notice and may appropriately be considered on a Rule 12(c) motion. *See supra*, n. 4.

[6] The text of the CFAA is set out in full at Appendix A.

A CFAA claim must be brought either (a) within 2 years of the date of the act of unauthorized access complained of or (b) assuming that act is not discovered right away, within 2 years of the date that the resulting damage from the act is discovered. Here, the "act complained of" is the alleged use of access to and use of information from his website. Egilman alleges that that act occurred in June 2001. Ver. Compl. ¶ 15. Egilman became aware of the "act complained of" no later than when the information was submitted to the court in Colorado in June 2001. He filed this Complaint, however, at the end of May 2004, long past the expiration of the statute.

As for his "discovery of the damage . . .," the only "damage" about which Egilman complains is that which flowed from the sanctions imposed on him by the *Ballinger* court: The "substantial legal fees" he incurred in appealing the sanction (Ver. Compl. ¶ 23), and the "damage to his reputation" resulting from having been sanctioned (Ver. Compl. ¶ 35). This means that Egilman "discovered the damage" no later than June 22, 2001, the date on which Egilman's false statement about Jones Day having bribed the *Ballinger* trial judge resulted in sanctions. Ver. Compl. ¶¶ 15, 16; *See* Ex. F, Sanctions Order.

Egilman alleges that he did not learn of the alleged involvement of Behr and, hence, K&H in providing a Jones Day attorney the username/password combination until November 2002 (Ver. Compl. ¶ 18). That, however, does not matter: Egilman was completely aware of both the acts and the purported damage resulting from those acts in June 2001. *See* Ex. C, Pl.'s Original Pet., at Section D. Based on his allegations, he was

obligated to bring any CFAA claim he thought he had no later than June 2003. In short, Egilman's CFAA claims are time barred.[7]

B. Egilman Has Not Suffered A Cognizable CFAA "Loss".

In addition to Egilman's CFAA claims being time barred, he also has failed to allege or demonstrate any "loss," as defined by the statute. The CFAA could not be clearer that a civil plaintiff must have a cognizable "loss" to prevail under ***any*** of the statute's provisions.

The CFAA requires that a civil plaintiff must demonstrate that the prohibited conduct involved "1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B)." 18 U.S.C. §1030(g).[8] Necessarily assuming that Egilman's action falls, if at all, under clause (i), he must, therefore, have suffered a "loss . . . aggregating at least $5,000 in value." 18 U.S.C. § 1030(a)(5)(B)(i).[9] "Loss," in turn, is defined to include the "any reasonable cost to the 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 "revenue lost, cost incurred, or

---

7 The overlapping Texas Action, which Egilman voluntarily dismissed, did not toll the CFAA statute of limitations. *See, e.g., York and York Const. Co. v. Alexander*, 296 A.2d 710, 712 (D.C. 1972) (general rule is that statute of limitations is not tolled by action voluntarily dismissed without prejudice).

8 This prerequisite for bringing a civil action, as well as the definition of "loss," were added by the USA PATRIOT Act, tit. VIII, § 814(e) & (d), 115 Stat. 272, 384 (2001).

9 Clearly, the other possible factors in (ii) through (v) (medical examination; physical injury; threat to public health or safety; government computer) do not apply.

other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11).

Egilman has suffered no such "loss." Although he alleges that Defendants' actions "caused . . . damages" in excess of $5,000 (Ver. Compl. ¶ 28), he does not allege that he has suffered any "losses" that, in any way, resemble the cost of responding to the offense, or restoring the data, program or system. Indeed, given that Defendants allegedly used a username/password combination that Egilman specifically intended to enable access to his website, there is, not surprisingly, no allegation that Egilman had any losses cognizable under the CFAA, such as expenses in "restoring" his computer. Neither his computer, nor his website nor any of the data on his website or otherwise stored in his computer could have been or were damaged in any way by Defendants' use of a valid username/password combination.

Instead, Egilman objects to the *use* of "information" from his website, allegedly to "besmirch" his "professional reputation and compromise the effectiveness of" his testimony. Ver. Compl. ¶ 17. *See also id.* ¶ 35 (reputational harm) and ¶ 23 (costs of appealing the sanctions order).[10] Even if, as pled, these are "consequential damages" from Defendants' conduct, the statute is clear that any such alleged "loss" must be due to an "interruption of service." 18 U.S.C. § 1030(e)(11). Egilman, however, is not

---

[10] Given the standards applicable to this motion, the Defendants do not contest the truth of these allegations at this stage of the case. Suffice it to say, however, that their silence should not be deemed acquiescence in the truth of Egilman's claims. Indeed, that the *Ballinger* court found that Egilman had violated the Court's Order and that this finding was affirmed, speak volumes about the lack of merit to such allegations.

complaining about that either. To the contrary, his Complaint alleges nothing about any harm to his computer or his website and nothing whatsoever about any loss he incurred as a result of any damage to his computer. He therefore did not suffer the requisite economic "loss" to his computer or his website. *Nexan Wires S.A. v. Sark-USA, Inc.*, 319 F. Supp. 2d 468, 475-77 (S.D.N.Y. 2004) (loss needs to be related to the computer, investigative costs incurred in determining damage, cost of remedying damage or costs incurred because computer service was "interrupted"; "lost revenue due to lost business opportunity" is not "loss" under CFAA); *Register.com Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238, 252 n. 12 (S.D.N.Y. 2000) (lost revenue and other consequential damage claims are permissible under the CFAA only if caused by impairment or unavailability of data; how the defendant uses the data once it is extracted from the computer is irrelevant), *aff'd*, 356 F.3d 393 (2d Cir. 2004).

C. Egilman's CFAA Claims Are Otherwise Defective.

The CFAA is principally a criminal statute but provides for civil actions in the limited circumstances described above. The statute has several provisions, including those prohibiting unauthorized access to government computers or obtaining governmental or financial information. There are only three provisions of the CFAA that even arguably might relate to the conduct alleged by Egilman: (1) unauthorized access to a computer with intent to defraud in order to further the fraud; (2) unauthorized access causing computer related damage and loss aggregating $5,000; and (3) trafficking in passwords or other information with the intent to defraud. 18 U.S.C. § 10301(a)(4),

(a)(5) & (a)(6). Egilman has not pled any facts that would support any claim under any of these provisions.

First, Egilman's allegation that "Defendants knowingly and with intent to defraud Dr. Egilman . . ." (Ver. Compl. ¶ 27) appears to be an attempt to invoke CFAA section 1030(a)(4). That provision prohibits a person from accessing a protected computer without authorization "knowingly and with intent to defraud . . . and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computers and the value of such use is not more than $5,000 in any one-year period." 18 U.S.C. § 1030(a)(4).

If that is the provision on which Egilman relies, however, his claim is defective. He alleges no facts demonstrating that K&H or Behr intended to "defraud" Egilman and that Behr's access to his website somehow furthered any "intended fraud." All Egilman alleges is that Defendants had access to Egilman's website and reviewed and obtained the "demonstrably false" material that Egilman, by his own admission, put there for unauthorized users to see and disclose. Ver. Compl. ¶¶ 14-17. There was nothing fraudulent in Behr's giving the username/password information to Jones Day, nor in the use of that material by Jones Day to enable it to alert the *Ballinger* court of Egilman's violation of the Court's Order and his defamation of the judge. Nor has Egilman even attempted to plead any such fraud.

Moreover, Egilman does not allege that Defendants obtained "anything of value." Indeed, the material obtained was, by Egilman's own admission, "demonstrably false" and, therefore, utterly without any commercial value to Egilman or anyone else. Thus,

this is not a case where a violator of CFAA gained unauthorized entry to a computer to obtain valuable, protected data.[11]

Second, to the extent Egilman somehow is attempting to invoke section 1030(a)(5), that provision also is not available to him. It prohibits intentional unauthorized access to a protected computer that causes both (1) damage (§ 1030(a)(5)(A)(iii)) and (2) a loss of at least $5,000 that results from the unauthorized access (§ 1030(a)(5)(B)(i)). Egilman has (as noted above) suffered neither "loss" nor any "damage," as defined in the CFAA. The "damage" Congress sought to punish is plain, given its emphasis on "impairment to the integrity or availability" of data or information that resides on a computer. 18 U.S.C. § 1030(e)(8). As one court put it, the purpose of the CFAA is to guard against "damage to computer systems and electronic information." *In re DoubleClick Privacy Litig.*, 154 F. Supp. 2d 497, 525 n. 34 (S.D.N.Y. 2001) (granting motion to dismiss CFAA claim for failure to allege facts demonstrating any cognizable "loss"). *See also Tyco Int'l Inc. v. Does*, No. 01 Civ 3856, 2003 U.S. Dist. LEXIS 11800, *4 (S.D.N.Y. 2003) (although CFAA allows for recovery beyond physical damage, "the additional types of damages . . . have generally been limited to those . . .

---

[11] Section 1030(a)(4) also prohibits computer hacking to obtain use of a computer to carry out a fraud, for, *e.g.*, using one person's computer for purposes of "spoofing" or otherwise masking the true identity of the perpetrator of the fraud. That prohibition also is plainly inapplicable to Defendants' conduct and, in any event, Egilman does not allege that the "object of the fraud" was Defendants' ability to obtain access to his computer in order to "use" it for some other illicit purpose.

necessary to assess the damage caused to the plaintiff's computer system or to resecure the system").

Egilman's discovery responses in the overlapping Texas Action confirm that the lost revenue, reputational damages, costs to appeal the Colorado court's Sanctions Order and related legal fees are the only damages for which Egilman seeks redress here. *See, e.g.*, Ex. J, Pl.'s Supplemental Resp. to Def. Req. to Pl. for Disclosure, at 4, *Egilman v. Jones, Day, Reavis & Pogue* (filed Dec. 19, 2003) (claiming damages for lost website revenue, damage to reputation, costs of appealing the Sanctions Order, and monetary damage caused by failure to "hold as confidential" downloaded material).[12] These simply are not cognizable as the types of damage that would support a CFAA claim.

Finally, to the extent Egilman might have meant to plead a claim under 18 U.S.C. § 1030(a)(6)(A), which imposes liability on anyone who "knowingly and with intent to defraud traffics. . . in any password . . . if . . . such trafficking affects interstate or foreign commerce," his allegations still fall short. Even assuming K&H and Behr "trafficked" in a password by giving it to Defendant Jones Day, there are, as noted above, no allegations supporting a claim that Defendants had any "intent to defraud" Jones Day, Egilman or any other person. Nor is there any allegation that any such trafficking had any effect on interstate or commence.

---

[12] Egilman repeatedly claimed these damages in response other discovery requests. *See e.g.*, Ex. K, Pl.'s Answer to Anne Leather's First Set of Interrogs., at Q.11.

For the reasons set out above, as a matter of law, Egilman may not, and does not, plead a CFAA claim.

II. Egilman Has No Claim Under The DMCA.

Egilman's second count is based on section 1201 et seq. of title 17, the so-called "black box" or anti-circumvention provisions of the DMCA. The Complaint does not specifically identify which of the three provisions of section 1201 Defendants are alleged to have violated, but it appears that Egilman contends they violated section 1201(a)(1).[13] This section prohibits the circumvention of any "technological measure that effectively controls access to" a copyrighted work. Egilman's allegation is that his website was effectively protected, even though access could be obtained by using the combination of the username "Brown" (the institution at which he taught) and the password "student" (among the most obvious passwords for individuals interested in visiting their teacher's

---

[13] Section 1201 has three substantive inter-related, provisions. Section 1201(a)(1) prohibits the act of circumventing so-called access control measures. Section 1201(a)(2) prohibits the trafficking in technologies, products and services that are primarily designed to or only have limited commercially significant purposes other than to circumvent, or are marketed for use in circumventing, such access control measures. Section 1201(b) prohibits the trafficking in technologies, products and services that are primarily designed, or only have limited commercially significant purposes other than, to circumvent, or are marketed for use in circumventing, technological measures that protect rights of copyright owners. Egilman has not alleged any facts with respect to Defendants having engaged in any "trafficking" in any technologies, products and services that have the requisite design, purposes or marketing needed to support a claim under either section 1201(a)(2) or section 1201(b). Accordingly, Egilman has not stated a DMCA claim under either of those subsections. The full text of the anti-circumvention provisions of the DMCA is set out in full at Appendix B.

website). *See* Ver. Compl. ¶¶ 16. Such an obvious combination of words is not the type of "technological measure" that "effectively controls access" that Congress had in mind when it enacted the DMCA.

In the words of the House Committee on the Judiciary at the time of congressional consideration of the DMCA, the express purpose of section 1201 is to implement international treaty obligations of the United States to prohibit "decoding the encrypted codes protecting copyrighted works, or engaging in the business of providing devices or services to enable others to do so." H.R. REP. No. 551, pt. 1, 105th Cong., 2d Sess. at 10 (1998). To that end, section 1201 makes unlawful the unauthorized disabling of digital controls or otherwise decrypting a protected work, such as a Digital Versatile Disc ("DVD"). *See, e.g., Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001). The difference between that type of covered conduct and the acts about which Egilman complains is plain.

In order to allege a violation of section 1201(a)(1), a plaintiff must contend that a defendant has "circumvent[ed] a technological measure that effectively controls access to a work protected" under the Act. 17 U.S.C. §1201(a)(1)(A). The words of the DMCA are both technical and precise. In order "to circumvent" a technological measure, one of the following activities must have taken place: The defendant must have "descramble[d]" or "decrypt[ed]" a scrambled or encrypted work, or otherwise taken some action to "avoid, bypass, remove, deactivate, or impair a technological measure." If the defendant has committed one of those acts, he then violates section 1201(a)(1) to the

extent that such act has been done "without the authority of the copyright owner." 17 U.S.C. §1201(a)(3)(A).[14]

It is clear that neither K&H nor Behr engaged in any unlawful circumvention under the DMCA. Egilman does not and may not allege that Defendants "descrambled" or "decrypted" anything because his purported protection did not rely on scrambling or encryption. Nor, by entering a working username/password combination, did Defendants "remove," "impair" or "deactivate" the protection Egilman used to protect his website.[15]

---

[14] In addition to the defendant having circumvented without authority, a violation of section 1201(a)(1) requires two predicate elements. First, the work at issue must be properly protected by copyright. Second, the technological measure "circumvented" by the defendant must "effectively control" access to that copyrighted work. Egilman alleges that his website "provides access to numerous copyrighted works" authored by him and stored on his computer (Ver. Compl. ¶ 10) and, similarly, that the works on his computer were adequately protected by copyright. Ver. Compl. ¶¶ 31 and 32. He also alleges that he used "technical [sic] measures" to restrict access to his website (Ver. Compl. ¶¶ 11 and 31), but he does not allege that these measures were at all "effective" in actually restricting such access. Although this motion does not turn on the sufficiency (or not) of those allegations, Defendants do not, for purposes of this motion or otherwise, concede that the facts, as alleged, satisfy these two elements of that claim.

[15] In the words of the Committee on the Judiciary, the "act of circumventing a technological protection measure put in place by a copyright owner to control access to a copyrighted work is the electronic equivalent of breaking into a locked room in order to obtain a copy of a book." H.R. REP. No. 551, pt. 1, 105th Cong., 2d Sess. at 17-18 (1998). The analogy between the act of circumvention and "breaking and entering" was endorsed by the Copyright Office soon after the introduction of the bill that became the DMCA. *See* Hearing Before the House Subcomm. on Courts and Intellectual Property on H.R. 2180 and H.R. 2281, 105th Cong., 1st Sess. ("Libraries, for example, typically purchase a physical copy such as a book to make available on-site . . . . The bill would continue this basic premise, allowing a copyright owner to keep a work under lock and key and to show it to others selectively. Section 1201 therefore has been analogized to the equivalent of ***a law against breaking and entering***.") (statement of Marybeth Peters, Register of Copyright, at 49) (emphasis

Most important, entering a valid username and password does not constitute "otherwise" "avoiding" or "bypassing" a "technological measure" that "effectively controls" access to a password-protected website. In fact, this argument was expressly rejected in *I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc.*, 307 F. Supp. 2d 521, 532 (S.D.N.Y. 2004). The court's analysis in *I.M.S.*, although arising out of circumstances where the password was obtained from an authorized user, is directly applicable:

> We agree that plaintiff's allegations do not evince circumvention as that term is used in the DMCA. Circumvention requires either descrambling, decrypting, avoiding, bypassing, removing, deactivating or impairing a technological measure *qua* technological measure. In the instant matter, defendant is not said to have avoided or bypassed the deployed technological measure in the measure's gatekeeping capacity. The Amended Complaint never accuses defendant of accessing the e-Basket system without first entering a plaintiff-generated password.
>
> More precisely and accurately, what defendant avoided and bypassed was *permission* to engage and move through the technological measure from the measure's author. Unlike the CFAA, a cause of action under the DMCA does not accrue upon unauthorized and injurious access *alone;* rather, the DMCA "targets the *circumvention* of digital walls guarding copyrighted material."
>
> * * *
>
> Defendant is alleged to have accessed plaintiff's protected website without plaintiff's authorization. Defendant did not surmount or puncture or evade any

---

added). Egilman's Complaint alleges, at best, that the Defendants used the right key to open the door to Egilman's website, or used the right combination for a combination lock, not that they broke the lock. That act – the use of a username/password combination that worked – simply is not the sort of "circumvention" prohibited by the DMCA.

technological measure to do so; instead, it used a password intentionally issued by plaintiff to another entity.

Id. at 532-33. (emphasis in original; footnotes omitted).

That the Defendants did not obtain the "Brown/student" combination from an authorized user does not distinguish this case from *I.M.S.*[16] Egilman had, in fact, allowed anyone using those two words to enter into his website. He did not make any attempt to ensure that the combination could only be known to or used by individuals who were his actual students enrolled at Brown University. Moreover, the words, both by themselves and in combination, are so obvious that even someone without any technical expertise or circumvention device could deduce them. Given the precise language of section 1201(a)(1) and the persuasive holding in *I.M.S.,* Egilman's DMCA claim also fails.

III. Egilman Has No Cause Of Action For Trespass Or For Any Other Common Law Tort.

his computer has been damaged or diminished in condition or value, or that his (or anyone else's) use of his computer has been impaired in any way. To the contrary, he contends now, as he did in the overlapping Texas Action, that it was the false statement he, himself, posted on his website, once brought to the Colorado court's attention, that "damage[d] . . . his reputation" (Ver. Compl. ¶ 34). This alone affected his future ability

---

[16] The lack of *authorization* to use a username/password combination is irrelevant with respect to whether Defendants engaged in any of the proscribed *acts* of circumvention. To violate the statute, as set out in section 1201(a)(3)(A), a defendant must have (1) "descrambled, decrypted, etc." *and* (2) done so without the authorization of the copyright owner.

to serve as a testifying expert and cost him money in the appeal of the Sanctions Order (Ver. Compl. ¶¶ 17, 23, 35). *See also* Ex. L, Pl.'s Resp. to Def. Req. to Pl. for Disclosure, at 4, *Egilman v. Jones, Day, Reavis & Pogue, et al.*, filed Aug. 11, 2003. These, however, are not the type of damages recognized by the tort of trespass. Egilman's trespass claim fails as a matter of law in any jurisdiction or under any cognizable theory and, accordingly, should be dismissed.

CONCLUSION

For the foregoing reasons, the Verified Complaint should be dismissed with prejudice.

Dated: Washington, D.C.
August 16, 2004

DEBEVOISE & PLIMPTON LLP

By_____
Jeffrey P. Cunard (D.C. Bar No. 362477)
John S. Martin
Bruce P. Keller

Attorneys for Defendants Keller and Heckman LLP and Douglas J. Behr
555 13th Street, N.W., Suite 1100E
Washington, D.C. 20004
202-383-8000

Of Counsel
Richard Leighton (D.C. Bar No. 7757)
Keller and Heckman LLP
1001 G Street, N.W.
Suite 500 West
Washington, D.C. 20001
202-434-4100