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

| | |
|---|---|
| HEALTHCARE ADVOCATES, INC.,<br><br>Plaintiff,<br><br>v.<br><br>HARDING, EARLEY, FOLLMER & FRAILEY; JOHN F.A. EARLEY, III, CHARLES L. RIDDLE, FRANK J. BONINI, JR., KIMBERLY TITUS, and JOHN DOES 1-5,<br><br>Defendants. | Civil Action No. 2:05-cv-03524-RK<br><br>Hon. Robert F. Kelly |

**PLAINTIFF HEALTHCARE ADVOCATES, INC.'S OPPOSITION TO DEFENDANT HARDING, EARLEY, FOLLMER & FRAILEY'S MOTION FOR SUMMARY JUDGMENT**

**McCARTER & ENGLISH, LLP**
Scott S. Christie
Peter J. Boyer
Mellon Bank Center
1735 Market Street, Suite 700
Philadelphia, Pennsylvania 19103

*Attorneys for Plaintiff*
*Healthcare Advocates, Inc.*

v.

## TABLE OF CONTENTS





v.

## TABLE OF AUTHORITIES

### FEDERAL CASES

**FEDERAL STATUTES**



**MISCELLANEOUS**

## PRELIMINARY STATEMENT

Defendant Harding, Earley, Follmer & Frailey ("HEFF") has moved for summary judgment on all remaining counts against it and the individual defendants (collectively, "Defendants") in the Second Amended Complaint (the "Complaint"): Count I - Digital Millennium Copyright Act ("DMCA"), Count II - Copyright Infringement, Count III - Computer Fraud and Abuse Act ("CFAA"), Count V - Trespass to Chattels, and Count VI - Conversion.[1] Healthcare Advocates has moved for partial summary judgment against Defendants on its DMCA and CFAA claims.

As set forth in greater detail below, summary judgment in favor of Defendants on the DMCA, copyright infringement and CFAA claims is unwarranted. In fact, for the reasons set forth in Plaintiff Healthcare Advocates, Inc.'s Memorandum of Law in Support of Motion for Partial Summary Judgment as supplemented herein, Healthcare Advocates is entitled to summary judgment on its DMCA and CFAA claims.

## STATEMENT OF FACTS

The relevant facts are set forth in detail in Plaintiff's Statement of Undisputed Material Facts in Support of its Motion for Summary Judgment, which is supported by the Declaration of Scott S. Christie with exhibits submitted in support of Plaintiff's Motion for Summary Judgment (the "First Christie Decl."), (collectively, "SOF"), as supplemented by the facts contained in the Declaration of Scott S. Christie ("Second Christie Decl.") submitted in support herewith. All of these facts are hereby incorporated by reference.

[1] Healthcare Advocates voluntarily dismissed Count IV - Civil Conspiracy and Count VII - Intrusion Upon Seclusion.

## ARGUMENT

### POINT I

### DEFENDANTS ARE NOT ENTITLED TO SUMMARY JUDGMENT ON HEALTHCARE ADVOCATES' COPYRIGHT INFRINGEMENT CLAIM

Summary judgment on the copyright infringement claim against Defendants is improper at this juncture because a material question of fact exists concerning Defendants' use of Healthcare Advocates' copyrighted web pages obtained without authorization from the digital collection of Internet Archive. While Defendants' known use of these web pages in the context of submission to the Court in the Underlying Litigation (as defined in the SOF) arguably may constitute fair use under the Copyright Act, it is far from certain that this is the only use Defendants made of the web pages.

Defendant Titus may have saved over one hundred historical web pages for the Healthcare Advocates Website to the local hard drive of the HEFF computer she utilized to access such web pages through the Wayback Machine in July 2003. SOF at ¶¶ 66, 71, 74 & 78. As a direct consequence of the spoliation of electronic evidence on the computer hard drives used by Defendants in accessing Healthcare Advocates' historical web pages, it is impossible to confirm whether these web pages were, in fact, saved to the hard drive of the computer used by Defendant Titus and, if so, to determine what uses HEFF made of the web pages. Had HEFF properly preserved this critical evidence, an examination of the relevant hard drive would have revealed such information.

The obligation to preserve evidence arises "when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation." Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 216 (S.D.N.Y. 2003). The duty to preserve documents and information "attach[es] at the time that litigation was reasonably



v.

anticipated." Id. at 217 ("While a litigant is under no duty to keep or retain every document in its possession . . . it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request.") (internal citation omitted).

HEFF admits that it was immediately aware that the conduct of its representatives in accessing and printing historical web page from the Healthcare Advocates Website on July 9, 2003 and July 14, 2003 might be relevant to Underlying Litigation. SOF at ¶ 88. As such, HEFF had a duty to preserve the hard drives of the computers used by its representatives to make such unauthorized accesses as of July 9, 2003 and July 14, 2003. Inexplicably, and despite a steady stream of requests to preserve the content of the hard drives of the HEFF computers, HEFF made no effort to do so until February 24, 2006, over two and one half years later. SOF at ¶¶ 89-97.

In light of HEFF's spoliation of this critical evidence, Healthcare Advocates will seek a variety of sanctions, including an adverse inference instruction at trial. Mosaid Technologies Inc. v. Samsung Elec. Co., Ltd., 348 F.Supp.2d 332, 335 (D.N.J. 2004); see also Bowman v. American Medical Systems, Inc., 1998 WL 721079, at *3 (E.D.Pa. Oct. 9, 1998). Because Healthcare Advocates is entitled to an adverse spoliation inference under the circumstances, summary judgment on the copyright infringement claim is inappropriate and Defendants' motion for such relief must be denied.



v.

## POINT II

## HEALTHCARE ADVOCATES IS ENTITLED TO SUMMARY JUDGMENT ON ITS CLAIM UNDER THE DIGITAL MILLENNIUM COPYRIGHT ACT

Defendants contend that they are entitled to summary judgment on Healthcare Advocates' claim pursuant to the DMCA. They assert there are no material facts disputing that (a) the robots.txt exclusion is not a "technological measure;" (b) the robots.txt exclusion did not effectively control access to the historical content of the Healthcare Advocates website in the digital collection of Internet Archive; (c) representatives of HEFF did not "circumvent" the robots.txt exclusion to gain access to the historical content of the Healthcare Advocates website in the digital collection of Internet Archive; and (d) Defendants' fair use of the historical content of the Healthcare Advocates website is an affirmative defense to liability under the DMCA. Not only are Defendants incorrect that summary judgment on the DMCA claim in their favor is appropriate but, in fact, Healthcare Advocates is entitled to summary judgment on its DMCA claim.

### A. Healthcare Advocates' archived website content constitutes a protected work.

Defendants have not disputed that (a) the content of the Healthcare Advocates website is copyrightable; (b) Healthcare Advocates secured valid copyright registrations for its website content extending back to 1998; and (c) Healthcare Advocates obtained these registrations prior to access to the historical content of the Healthcare Advocates website in the digital collection of Internet Archive in July 2003. Thus, there is no genuine issue of material fact as to Healthcare Advocates' historical website content constituting a protected work under the Copyright Act.



v.

### B. The robots.txt exclusion is a technological measure

Defendants do not meaningfully contest that the robots.txt exclusion is a "technological measure" under the DMCA. Their token opposition amounts to the conclusory statement "robots.txt does not constitute 'a technological measure,' 'effective' or otherwise," Defendants' Memorandum of Law in Support of Motion for Summary Judgment ("Defs. Bf.") at 21, coupled with the observation that no reported decision has yet to address whether the robots.txt exclusion is a "technological measure" for DMCA purposes. Id. at 22 n.14. Such an effort does not in the least serve to negate the reality, as evidenced by Google's August 3, 2006 agreement with the University of California (First Christie Decl., Ex. J), that the robots.txt exclusion qualifies as a DMCA "technological measure," and the Court should so find.

### C. The robots.txt exclusion effectively controls access to copyright-protected website content in the custody of Internet Archive

Defendants contend that the robots.txt exclusion fails to "effectively control access" because (a) robots.txt is not a mandatory prohibition, but a voluntary protocol; (b) a supposed admission by a representative of Internet Archive that the robots.txt exclusion "does not even function;" and (c) there is no "password or other code" that qualifies as the "application of information, or a process or a treatment" allowing third parties to neutralize the blocking effect of this security mechanism.

As an initial matter, Defendants point to the voluntary nature of the robots.txt exclusion in a misguided attempt to argue that it is not effective. They contend that because some crawlers do not honor this exclusion, it cannot effectively control access to copyright-protected works. In support of their position, they quote out of context from a law review article for the proposition that a robots.txt exclusion is not an effective access control measure. Defs. Bf. at 23-24.

Defendants' misdirection is unavailing, however, because the focus here is not whether the robots.txt exclusion is or was universally recognized, honored or implemented. Rather, the appropriate analysis is whether during July 2003, the robots.txt exclusion was effective in preventing third party access to historical website content in the digital collection of Internet Archive. The undisputed facts clearly demonstrate the effectiveness of the robots.txt exclusion as directed to Internet Archive.

Although the robots.txt exclusion is discretionary, Internet Archive elected to treat it as mandatory. SOF at ¶ 34. During July 2003, as long as a website computer server contained a Robots Text String customized to communicate with the Internet Archive Crawler, Internet Archive blocked public access to historical web page content of this website. SOF at ¶¶ 29, 34, 36 & 37. The computer server hosting the Healthcare Advocates Website contained such a Robots Text String on July 9, 2003 and on July 14, 2003. SOF at ¶¶ 37, 40 & 43. Healthcare Advocates reasonably believed that its historical website content was rendered inaccessible to the public. SOF at ¶ 38. In fact, in the normal course of its operation at Internet Archive, the robots.txt exclusion was very effective in blocking access to archived web page content, including copyright-protected content. SOF at ¶ 39.

Defendants' efforts to bolster their tortured reasoning with a law review article are equally unavailing. They point to the quote: "Ignoring a robot exclusion or avoiding an IP block does not violate the [DMCA], because neither implicates an access control measure," Maureen A. O'Rourke, *Shaping Competition on the Internet: Who Owns Product and Pricing Information?*, 53 VAND. L. REV. 1965, n.102 (2000), and argue that this is synonymous with their view that the robots.txt exclusion is not an effective access control device here. Defendants' fail to acknowledge that this quote was made by the author in the context of an



v.

environment where honoring the robots.txt exclusion is voluntary. See id. at 1989-90. If the robots.txt exclusion is merely advisory and an individual seeking access to web page content ignores that protocol, one can hardly disagree with the conclusion that the robots.txt exclusion does not effectively control access under these circumstances. See id. On the other hand, where, as here, the robots.txt exclusion is a mandatory provision that, when implemented by a website owner, serves as a barrier for all requested accesses to historical website material in the digital collection of Internet Archive, this security mechanism constitutes an effective access control device, circumvention of which is a violation of the DMCA. See id. at 1990.

Furthermore, the Defendants argue that Gordon Mohr, a representative of Internet Archive, admitted that the robots.txt exclusion "does not even function." Defs. Bf. at 24. Contrary to the Defendants' fanciful suggestion, Mr. Mohr never made such an admission or anything remotely similar. The Defendants again take out of context language which is not a commentary on the effectiveness of the robots.txt exclusion in preventing access to copyright-protected historical web pages in Internet Archive's digital collection. Rather, it speaks to a procedure at Internet Archive to limit the frequency with which Internet Archive computers check the robots.txt file of a computer server for a denial string in response to a request by a third party for historical web page content for that website. Deposition of Gordon Mohr ("Mohr") at 107 (Second Christie Decl., Ex. A). To conserve scarce computing resources, these Internet Archive computers were programmed to check a website's robots.txt file for a denial string no more frequently than once every 24 hours. Id. During the period from July 9, 2003 through July 14, 2003, this once-per-day checking mechanism did not function on a few of these Internet Archive computers. Id. This "glitch" in the once-per-day checking mechanism simply caused the Internet Archive computers to check a website's robots.txt file each and every time a request

was made for that website's historical content as opposed to relying upon a locally-stored copy for at least 24 hours. Id. at 108 & 113-115. It did not have any impact upon the effectiveness of the robots.txt exclusion itself. Id. at 108.

Finally, the Defendants' argue that the robots.txt exclusion does not effectively control access to copyright-protected materials because it fails to meet the appropriate statutory definition. The DMCA provides that:

> a technological measure "effectively controls access to a work" if the measure in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.

17 U.S.C. § 1201(a)(3)(B). Defendants contend that the robots.txt exclusion is merely a passive blocking mechanism, not a dynamic access control mechanism as required by this definition.

In support of their view, the Defendants rely exclusively upon an analogy to the non-precedential district court decision in Agfa Monotype Corp. v. Adobe Systems, Inc., 404 F.Supp.2d 1030 (N.D.Ill. 2005). In that case, Agfa, an owner of copyrighted text fonts, sued Adobe under the DMCA claiming that Adobe's popular software program Acrobat 5.0 allowed individuals to view and edit the text of documents in Agfa's copyrighted fonts without authorization from Agfa and, in the process, bypass prohibitions on such use spelled out in licensing rights embedded with the font in embedding bits. Id. at 1031 & 1036. These embedding bits travel with the electronic document and communicate with software programs like Adobe Acrobat, indicating the licensing rights for viewing, editing and copying that the owner of each font has granted. Id. at 1031. However, an embedding bit cannot be read by a software program until after that program has already accessed the data file for the corresponding font. Id. Indeed, the font data file can be accessed by a software program regardless of the



v.

permissions contained within the corresponding embedding bit. Id. A software program need not complete any authorization sequence whatsoever to gain access to a font. Id.

The Agfa court ruled that embedding bits did not "effectively control access" to the fonts as mandated by the statutory definition. Id. at 1036-37. First, an embedding bit was entirely passive insofar as it merely broadcast font licensing rights to software programs. Id. at 1036. There was no element of interaction with or manipulation of an embedding bit necessary to achieve access to the font data files. Id. Second, an embedding bit did not even control access to the corresponding font data file because this data file was accessible despite the existence of an embedding bit containing a licensing restriction on viewing, editing and copying. Id. An embedding bit did not serve as a component of the authorization sequence; it was not a digital wall that must be breached in order to obtain access. Id.

For the purpose of analysis under the DMCA, a robots.txt exclusion is markedly different from an embedding bit. A robots.txt exclusion is a text string that a website owner inserts into a file names "robots.txt" on the computer server hosting the website. SOF at ¶29. It serves as an access control device directed to a crawler seeking content of the website. SOF at ¶27. The robots.txt exclusion communicates with these crawlers, directing whether or not they have the permission of the owner of the website to access and copy the content of the website. SOF at ¶30. A Robots.txt Text String can be configured by a website owner to communicate with all web crawlers or only to particular web crawlers. SOF at ¶31. Likewise, a Robots.txt Text String can be modified by a website owner to deny a specific crawler permission to access and copy all content of a website or just a certain potion of that website content. SOF at ¶32.

In July 2003, the Internet Archive Crawler did not access and copy and Internet Archive did not make publicly available web page content from the current versions of websites that



v.

contained a robots.txt exclusion directed to the Internet Archive Crawler. SOF at ¶35. Furthermore, Internet Archive also excluded from public access existing archived web page content of websites that contained a robots.txt exclusion directed to the Internet Archive Crawler. SOF at ¶36. Indeed, in the normal course of its operation at Internet Archive, a robots.txt exclusion, depending upon its configuration, consistently prevented access to some or all of a website's content in response to a third party request for that content. See SOF at ¶¶33-39.

Unlike an embedding bit, a robots.txt exclusion was a true access control device as applied to Internet Archive. It was a filter through which all third party inquiries for website content passed. Before Internet Archive produced any archived web page content in response to a public inquiry through the Wayback Machine, it first checked the live version of the website to determine whether a robots.txt exclusion was in place. If no robots.txt exclusion was present, access to the archived content was granted. If a robots.txt exclusion existed, Internet Archive denied access to the extent directed by the robots.txt exclusion. In contrast to an embedding bit, a robots.txt exclusion served as the gatekeeper in the authorization sequence for access to archived web page content

Moreover, as opposed to an embedded bit, a robots.txt exclusion was more than just a passive communicator of access permissions. An embedded bit is a fixed and unchanging grant or refusal to grant access to a particular font that travels with an electronic document as it transverses the Internet. It is an on/off switch stuck in one position for eternity. In contrast, a robots.txt exclusion was dynamic. The robots.txt exclusion resided on the computer server hosting the website and was easily accessible to and manipulable by the website owner. It could be configured at will by the website owner to allow access only to a discrete portion of the web page content. It also could be removed entirely by the website owner to facilitate unfettered



v.

access to the website material. This ability to modify or remove a robots.txt exclusion by the copyright owner was the "process or treatment" required by statute to "effectively control access."

During the period from July 9, 2003 through July 14, 2003, the robots.txt exclusion did indeed effectively control access to the historical web page content of the Healthcare Advocates Website in the digital collection of Internet Archive. There is no genuine issue of material fact to the contrary.

**D. Defendants repeatedly circumvented the robots.txt exclusion protecting Healthcare Advocates' historical web page content.**

Defendants appear to contend that because the Complaint narrowly alleges they circumvented the robots.txt exclusion through "hacking" and because there is no evidence obtained through discovery that representatives of HEFF engaged in "hacking" to obtain access to the historical content of the Healthcare Advocates website in the digital collection of Internet Archive, Defendants did not circumvent the robots.txt exclusion.

Contrary to Defendants' contention, the Complaint does not allege circumvention through "hacking." Rather, the Complaint closely tracks the language of the statute, alleging defendants "knowingly, willfully and intentionally circumvented and caused to be circumvented the denial text string in the robots.txt file on the computer server hosting the **www.healthcareadvocates.com** web site on at least 92 separate occasions on July 9, 2003 and July 14, 2003." Second Amended Complaint at ¶ 75.

Furthermore, there are no factual allegations in the Complaint that Defendants engaged in "hacking." The only appearance of the terms "hacking," "hacks" or "hacker" in the Complaint are in the section headings of that document which merely summarize, for the convenience of the



v.

reader, the essence of the factual allegations to follow. The section headings of the Complaint do not constitute factual allegations and have no probative value in and of themselves.

However, even if use of the term "hacking" and derivations thereof in the section headings of the Complaint had any significance in Healthcare Advocates' pleading of its DMCA claim, that term accurately describes Defendants' conduct. There is not one generally accepted definition of the term "hacking;" it is defined differently in different contexts. Deposition of Edward Felten ("Felten") at 133 (Second Christie Decl, Ex. C); Mohr at 198-199 (Second Christie Decl., Ex. A). One common connotation of "hacking" is "unauthorized access." Felten at 134 (Second Christie Decl, Ex. C); Mohr at 199 (Second Christie Decl., Ex. A). Defendants' conduct here may be accurately categorized as "hacking" to the extent this term implies unauthorized access. Mohr at 199 (Second Christie Decl., Ex. A); Flynn at 184 (Second Christie Decl., Ex. B). Indeed, that is the context in which this term is employed in the Complaint. "Hacking" and "unauthorized access" consistently have been synonymous in the manner that Healthcare Advocates' DMCA claim was pleaded; "unauthorized access" is not a new theory or an alternative approach to this claim. See Defs. Bf. at 20.

In a further effort to unnecessarily cloud the issue, Defendants seem to assert that in the context of proving its DMCA claim, Healthcare Advocates improperly focuses on Defendants' "unauthorized access" to its historical website content rather than "unauthorized use" of that material after it was accessed. As set forth in greater detail below, Defendants' use of the historical website content, whether authorized or not under copyright law, has no bearing on the DMCA claim. The focus of the DMCA claim is penetrating the protective mechanism securing the copyrighted material in the first instance; Defendants use of the historical web pages thereafter is irrelevant. Circumvention of the robots.txt exclusion cannot be established without



v.

demonstrating "unauthorized access" to the historical website content. Stated somewhat differently, if Defendants' access was authorized there would be no circumvention. Accordingly, Healthcare Advocates' focus upon Defendants' "unauthorized access" is appropriate and necessary in establishing its entitlement to a judgment in its favor on its DMCA claim.

There are no genuine issues of material fact in dispute as to Defendants' intentional circumvention of the robots.txt exclusion to gain access to Healthcare Advocates' historical website content.

**E. The fair use defense under the Copyright Act is inapplicable to negate liability under the anti-circumvention provision of the DMCA.**

Defendants' attempt to invoke the Copyright Act's fair use defense in connection with the DMCA claims asserted against them is unavailing and Defendants' motion for summary judgment on this ground likewise should be denied.

The language of the DMCA is clear and the foremost commentator on copyright law and the author of the most authoritative treatise on the subject, *Nimmer on Copyight*, said it best: "[T]here is no such thing as a section 107 fair use defense to a charge of a section 1201 violation" under the DMCA. David Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L.REV. 673, 723 (2000).

Furthermore, the legislative history of the DMCA and "the better policy view supports the simple conclusion that, except as incorporated in the exceptions to liability stated in the statute, DMCA liability is not liability for copyright infringement and does not hinge on the presence or absence of fair use or other defenses to an infringement claim." Raymond T. Nimmer, Information Law § 4:35 (2006). As evidenced by the text of Section 107 of the Copyright Act, Congress knows how to craft a fair use exception and obviously could have

included such a provision in the subsequently-promulgated DMCA, yet elected not to do so. Indeed, Congress, in enacting the DMCA, explicitly considered inclusion of a blanket fair use exception to the DMCA's anti-circumvention and anti-trafficking provisions, but ultimately declined to add one. See H.R. Rpt. 105-551 pt. 2 at 25-26 (July 22, 1998) (noting concern about impact of anti-circumvention provisions on public's ability to make fair use of copyrighted materials); see id. at 86 (rejection of proposal for fair use exception).

To the contrary, Congress added narrowly tailored fair use exemptions for nonprofit libraries, archives and educational institutions, reverse engineering and encryption research among other specific statutory exceptions. See 17 U.S.C. § 1201(d)-(j). Congress also implemented a mechanism intended to protect the public's ability to make non-infringing uses of protected works within the framework of the DMCA on an ongoing basis. See 17 U.S.C. § 1201(a)(1)(B)-(D) (vesting power in the Library of Congress to create exceptions from anti-circumvention liability for entities whose ability to make non-infringing use of certain types of works is negatively impacted by the anti-circumvention provisions of the DMCA). These prophylactic measures were in lieu of incorporating a general fair use exception to the DMCA.

Moreover, the "better approach to the fair use question" is that adopted by the Second Circuit in Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001). Raymond T. Nimmer, Information Law § 4:35 (2006); see also Universal City Studios, Inc. v. Reimerdes, 111 F.Supp.2d 294 (S.D.N.Y. 2000); 321 Studios v. Metropolitan Goldwyn Mayer Studios, Inc., 307 F.Supp.2d 1085 (N.D.Cal 2004); United States v. Elcom Ltd., 203 F.Supp.2d 1111 (N.D.Cal 2002).

Defendants in Corley appealed the lower court's entry of a permanent injunction on plaintiff's DMCA claims barring defendants from posting on the Internet or otherwise



v.

disseminating a program that decrypted digitally encrypted films on DVDs. See Corley, 273 F.3d at 443. Defendants argued on appeal, among other things, that Section 1201(c)(1) of the DMCA made the fair use defense to copyright infringement applicable to claims under the DMCA and that the DMCA, as interpreted by the District Court, was unconstitutional because it "eliminate[d] fair use of copyrighted materials." Id. at 458.

The Corley Court rejected defendants' contention that the DMCA's "savings clause," contained in Section 1201(c)(1), permits circumvention of a technological measure where the protected material "will be put to 'fair uses.'" Corley, 273 F.3d at 443. Section 1201(c)(1) provides "[n]othing in this section shall affect rights, remedies, limitations or defenses to copyright infringement, including fair use, under this title." Id. The Second Circuit rejected defendants' reading of this provision as creating a fair use exception to the DMCA and concluded that Section 1201(c)(1) "simply clarifies that the DMCA targets the *circumvention* of digital walls guarding copyrighted material (and circumvention tools), but does not concern itself with the *use* of those materials after circumvention has occurred. Id. (emphasis in original). The court explained that this section of the DMCA "ensures that the DMCA is not read to prohibit the 'fair use' of information just because that information was obtained in a manner made illegal by the DMCA." Id.

In rejecting Defendants' position, the Second Circuit noted that the legislative history of the DMCA "clearly refuted" Defendants' reading of Section 1201(c)(1). Id. at 444. The court referred to Congress' intent to balance "piracy and fair use concerns, eschewing the quick fix of simply exempting from the statute all circumventions for fair use." Id. at n.13. The Second Circuit noted the specific and limited exemptions for fair use included in the DMCA and reasoned that "[i]t would be strange for Congress to open small carefully limited windows for



v.

circumvention to permit fair use in subsection 1201(d) if it then meant to exempt in subsection 1201(c)(1) any circumvention necessary for fair use." Id. (emphasis in original).

The Second Circuit also rejected defendants' argument concerning a constitutional right to make fair use of copyrighted materials. Id. at 459. The court noted that no legal authority exists to support the conclusion that such a constitutional right exists. Id. In so holding, the Second Circuit explained that "[f]air use has never been held to be a guarantee of access to copyrighted material in order to copy it by the fair user's preferred technique or in the format of the original." Id.

Defendants rely upon Chamberlain Group, Inc. v. Skylink Technologies, Inc., 381 F.3d 1178 (Fed. Cir. 2004), cert. denied 2005 WL 218463 (2005), and Storage Technology Corp. v. Custom Hardware Engineering & Consulting, Inc., 421 F.3d 1307 (Fed. Cir. 2005) to support their argument that the fair use defense to copyright infringement applies to an anti-circumvention claim under the DMCA. Neither of these cases, however, provides the necessary foundation for this position.

Chamberlain involved a claim under the anti-trafficking provision of the DMCA, not the anti-circumvention provision which is applicable here. Defendants liberally quote from that decision yet, almost as an afterthought, acknowledge that the court specifically declined to rule whether the § 107 fair use defense was applicable to the DMCA. Chamberlain, 381 F.3d at 1199 n.14. In so doing, however, the Chamberlain court hinted that a fair use defense was confined to the realm of the Copyright Act and not cognizable under the DMCA. Id. ("[W]e note only that though the traditional fair use doctrine of § 107 remains unchanged as a defense to copyright infringement under § 1201(c)(1), circumvention is not infringement.").



v.

Inexplicably, Storage Technology, relying solely upon Chamberlain, somehow defied all logic by jumping to the conclusion that infringement, and thus the fair use defense, is applicable to an anti-circumvention claim under the DMCA. Storage Technology, 421 F.3d at 1318. The Storage Technology court, citing page 1203 of Chamberlain, ruled that "[a] copyright owner alleging a violation of section 1201(a) consequently must prove that the circumvention of the technological measure either 'infringes or facilitates infringing a right protected by the Copyright Act.'" A review of the source of that quote on page 1203 of Chamberlain reveals that that court determined such an element is required solely for an anti-trafficking claim under Section 1201(a)(2); there is no discussion whatsoever in Chamberlain extending that element to an anti-circumvention claim under Section 1201(a)(1). Indeed, unlike the Storage Technology court, the Agfa court understood that Chamberlain, through this operative language, only "interpreted Section 1201(a)(2) liability." Agfa, 404 F.Supp.2d at 1034-35. The Storage Technology court's contradictory conclusion is unfounded and unsupported.

The plain language of the DMCA, its legislative history, the sage opinion of David Nimmer, and the persuasive reasoning of the Second Circuit in Corley all support the view that a fair use defense is inapplicable to an anti-circumvention claim under the DMCA. Chamberlain and Storage Technology offer no persuasive authority to the contrary. The Court should rule that fair use is not a cognizable defense to this DMCA claim.

## POINT III

## HEALTHCARE ADVOCATES IS ENTITLED TO SUMMARY JUDGMENT ON ITS CLAIM UNDER THE COMPUTER FRAUD AND ABUSE ACT

Defendants contend that they are entitled to summary judgment on Healthcare Advocates' claim under the CFAA. They argue that there are no material facts in dispute that (a)



v.

HEFF did not exceed authorized access when reviewing and copying historical web page content in the digital collection of Internet Archive; and (b) Healthcare Advocates failed to demonstrate at least $5,000 of economic loss flowing from HEFF's conduct in a one-year period. Summary judgment in favor of Defendants on the CFAA claim is not warranted. Indeed, Healthcare Advocates is entitled to summary judgment on its CFAA claim.

**A. Defendants exceeded authorized access to Internet Archive's computer servers storing its digital collection of web page content.**

Defendants clearly exceeded their authorized access of Internet Archive's computer servers in accessing historical web page content of the Healthcare Advocates Website. See Plaintiff Healthcare Advocates, Inc.'s Memorandum of Law in Support of Motion for Partial Summary Judgment at III.A. Recognizing that the undisputed facts support this position, Defendants again take out and dust off the fair use defense, improbably claiming that it somehow negates any access in excess of authorization.

Contrary to Defendants' unsupported assertions, the fair use defense to a claim for copyright infringement does not provide a defense to a claim under the CFAA. Most notably, Defendants fail to cite any authority to support their reliance upon this defense in the context of the CFAA. Indeed, our research has not revealed a single case to support Defendants' position.

Fair use, previously a common law defense to copyright infringement, is codified in Section 107 of the Copyright Act. 17 U.S.C. § 107. The promulgation of the CFAA post-dates the Copyright Act. The CFAA itself does not contain a fair use defense, nor does it by reference incorporate the fair use defense set forth in Section 107 of the Copyright Act. Had Congress intended application of the fair use defense to claims under the CFAA, Congress certainly would have crafted the CFAA accordingly.



v.

As with the DMCA claim, the fair use defense has no place here. There is no genuine issue of material fact as to HEFF exceeding authorized access of Internet Archive's computer servers in accessing historical web page content of the Healthcare Advocates Website.

**B. Through its intentional exceeding of authorized access, Defendants obtained information from a protected computer through an interstate communication.**

Defendants have not contested that (a) the computer servers housing Internet Archive's digital collection of web page content qualify as protected computers; (b) they repeatedly accessed and printed historical web page content of the Healthcare Advocates Website from Internet Archive's computer servers; and (c) all of Defendants' accesses to the computer servers housing Internet Archive's digital collection of web page content were accomplished by virtue of an interstate communication between Pennsylvania and California. Therefore, there is no genuine issue of material fact as to these elements of the CFAA claim

**C. Defendants' conduct caused a loss during a 1-year period aggregating at least $5,000 in value.**

Defendants argue that Healthcare Advocates has failed to demonstrate more than $5,000 in cognizable losses during a one-year period. The term "loss" is defined by statute to include "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, systems, 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). To the contrary, Healthcare Advocates sustained economic losses that far exceed the $5,000 threshold pursuant to the CFAA.

Healthcare Advocates assists the public in securing, paying for, and receiving reimbursement for necessary health care, and Healthcare Advocates had a credit card database on its website, as well as a portion of the site dedicated to members only. See Flynn Dep. at 11; 151



v.

- 152 (Second Christie Decl., Ex. B). Consequently, Healthcare Advocates does business in the highly sensitive field of health care and insurance, which often involves a host of privacy issues, including but not limited to compliance with the federal Health Insurance Portability and Accountability Act ("HIPAA"). When Defendants exceeded their authorized access of Internet Archives' computer servers in accessing historical web page content of the Healthcare Advocates Website, Defendants could potentially have viewed or distributed information from those historical web pages, or the then-current version of the Healthcare Advocates Website, that relate to Healthcare Advocates' customers. After Defendants' unauthorized acts occurred, Healthcare Advocates was forced to investigate whether a security breach to its data occurred and to conduct a damage assessment by determining its duties to customers resulting from the breach.

The fact that Healthcare Advocates was not the owner of the compromised computers is irrelevant to whether or not it sustained losses, since "the statute does not restrict consideration of losses to only the person who owns the computer system." U.S. v. Millot, 433 F.3d 1057, 1061 (8th Cir. 2006) (finding district court properly instructed jury to consider losses sustained by party that did not own the computer system accessed, in determining whether statutory minimum was met under CFAA); Theofel v. Farey-Jones, 341 F.3d 978, 986 (9th Cir. 2003) ("[i]ndividuals other than the computer's owner may be proximately harmed by unauthorized access, particularly if they have rights to data stored on it").

Furthermore, Healthcare Advocates' quantum of damages are not diminished because certain types of damage, such as physical damage to the computer system or data, did not occur. See Kaufman v. Nest Seekers, LLC, 2006 WL 2807177 at *8 (S.D.N.Y. September 26, 2006) (finding loss claimed by plaintiffs in investigating potential damage to computer system and website was not lessened "merely because fortuitously no physical damage was allegedly caused



v.

to the computer system or software"); E.F. Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 585 (1st Cir. 2001) (finding loss suffered by plaintiffs in expending substantial sums to assess whether website was damaged was not lessened because no damage occurred); see also Pacific Aerospace & Electronics, Inc. v. Taylor, 295 F.Supp.2d 1188, 1197 (E.D.Wash. 2003) ("[t]he Explorica decision confirmed that any losses stemming from the unauthorized conduct are recoverable, as long as, in the aggregate, they meet the $5,000 threshold specified in the CFAA").

As an initial matter, Defendants do not contest that the following economic harm suffered by Healthcare Advocates is recognized and compensable under the CFAA:

a. Mr. Flynn's purchase of a data privacy and security treatise in late 2003 for $250 to assist in determining Healthcare Advocates' legal obligations as a consequence of Defendants' conduct;

b. Mr. Flynn's meeting in 2003 with an attorney specializing in the area of cyber law to determine corporate duties regarding client notification and related issues at a cost of $200;

c. A fee of $50 paid to HEFF in connection with serving a subpoena upon the firm to testify about the access of historical web pages from the Healthcare Advocates Website through the Wayback Machine by representatives of HEFF in July 2003;

d. A loss of $200 because the software program QuickBooks was rendered useless by virtue of Healthcare Advocates' removal of its customer credit card database from the Healthcare Advocates Website as a direct response to the access of historical web pages from the Healthcare Advocates Website through the Wayback Machine by representatives of HEFF in July 2003; and

e. The incremental cost of approximately $50 per year from July 2003 forward for U.S. postage to mail sensitive information rather than send it via e-mail due to concerns about potential breaches of security raised by the access of historical web pages from the Healthcare Advocates Website through the Wayback Machine by representatives of HEFF in July 2003.

SOF at ¶76(b), (c), (f), (g) & (i). Defendants affirmatively acknowledge that Healthcare Advocates has sustained $887.50 in economic damages, $750 of which was incurred during the period July 2003 through July 2004.



v.

Moreover, Defendants implicitly concede that even more of Healthcare Advocates' claimed expenses are appropriate. Defendants are accepting of the principle that expenses incurred by Healthcare Advocates to determine its legal obligations and corporate duties as a result of Defendants' conduct are legitimate. SOF at ¶76(b) & (c). Accordingly, they cannot quarrel with the legitimacy of the approximately 160 hours Mr. Flynn[2] spent in 2003, valued at between $10,000 and $16,000, for these same purposes.[3] See SOF at ¶76(a). Likewise, if the $50 witness fee to HEFF from service of a subpoena in the Underlying Litigation seeking testimony related to Defendants' conduct counts, so to does other legal fees and costs in the Underlying Litigation incurred for the same general purpose, including Healthcare Advocates' motion to amend the complaint. Compare SOF at ¶76(f) with SOF at ¶76(d).

Defendants mischaracterize Healthcare Advocates' claim of certain legal fees and expert witness costs, contending that the company is attempting to improperly pad its CFAA expenses. Healthcare Advocates is not seeking to qualify all legal fees and costs incurred in both the Underlying Litigation and this case as compensable damages. Instead, it seeks only those reasonable fees and costs narrowly tailored to assessing the nature, extent and degree of harm caused by Defendants' conduct. More precisely, Healthcare Advocates' fees and costs for responding to Defendants' conduct and gathering the information required to conduct a meaningful damage assessment are reimbursable under the CFAA despite the fact that they happen to have been incurred in the litigation context. See 18 U.S.C. § 1030(e)(11); see also EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 585 (1st Cir. 2001) (loss under CFAA

[2] The fact that Mr. Flynn is an employee of Healthcare Advocates and not an outside contractor is irrelevant to the determination of Healthcare Advocates' losses. See U.S. v. Middleton, 231 F.3d 1207, 1214 (9th Cir. 2000) ("[t]here is no basis to believe that Congress intended the element of 'damage' to depend on a victim's choice whether to use hourly employees, outside contractors, or salaried employees to repair the same level of harm to a protected computer"); U.S. v. Millot, 433 F.3d 1057, 1061 (8th Cir. 2006).

[3] Contrary to Defendants' unsupported assertion, Mr. Flynn was not "conduct[ing] legal research with respect to the issues relevant to his company's claim." Defs. Bf. at 42.



v.

includes remedial and investigative expenses incurred by plaintiff); Physicians Interactive v. Lathian Systems Inc., 2003 WL 23018270 at *6 (E.D.Va. Dec. 5, 2003) (finding plaintiff likely to succeed on merits of CFAA claim where plaintiff stated in affidavit that it "spent in excess of approximately $18,750 to assess the extent" of defendants' alleged attacks on plaintiff's website); I.M.S. Inquiry Management Systems, Ltd. v. Berkshire Information Systems, Inc., 307 F.Supp.2d 521, 525 (S.D.N.Y. 2004) (finding plaintiff adequately pled loss element under CFAA by alleging defendant's unauthorized access of plaintiff's web-based advertisement tracking service forced plaintiff to incur costs of more than $5,000 in damage assessment and remedial measures); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F.Supp.2d 1121, 1126-27 (W.D.Wash. 2000).

For the Underlying Litigation, cognizable fees and costs are those related to subpoenaing a representative of HEFF to testify about Defendants' conduct, Healthcare Advocates' motion to amend the complaint to add HEFF as a defendant due to Defendants' conduct, and any other expenditures that would not have been incurred but for Defendants' conduct. See SOF at ¶76(d) & (f). Reimbursable fees and costs from this case are not those generally related to the litigation process against Defendants. Rather, they center around efforts to secure from Internet Archive information uniquely within its possession, custody and control, including relevant Internet Archive web logs, to facilitate an understanding of the nature, extent and significance of Defendants' conduct as well as the assistance of computer forensic experts to analyze and interpret the Healthcare Advocates and Internet Archive web logs to help achieve this same understanding. See SOF at ¶76(e) & (h).

In 2005, prior to filing this lawsuit, Healthcare Advocates retained consulting computer forensic expert Warren Kruse and incurred $5,000 in expenses having him analyze and interpret



v.

just the Healthcare Advocates web logs related to Defendants' conduct. See SOF at ¶76(h); Second Christie Decl. at ¶2. Without the corresponding web logs from Internet Archive, his analysis and conclusions were limited. Id.

Beginning at least as early as May 2005, Healthcare Advocates approached representatives of Internet Archive in an effort to obtain the Internet Archive web logs related to Defendants' conduct and related assistance from Internet Archive personnel. Id. at ¶3. Representatives of Internet Archive advised at that time that the relevant web logs no longer existed and, furthermore, declined to provide any other assistance to Healthcare Advocates related to clarifying the nature, extent and significance of Defendants' conduct. Id. Because such information and assistance was critical to Healthcare Advocates' ability to conduct a meaningful damage assessment, Healthcare Advocates believed that it had no other meaningful alternative other than to name Internet Archive as a defendant in this case. Id.

In the original complaint in this case filed July 8, 2005, Healthcare Advocates sued not only Defendants, but also Internet Archive for failing to adequately secure the historical web pages of the Healthcare Advocates Website in its digital collection. Id. at ¶4. On two separate occasions, Internet Archive unsuccessfully moved to dismiss the complaint. Id. It was only after the Court denied the second motion to dismiss, forcing Internet Archive to respond to Healthcare Advocates' interrogatories and document production requests, that Healthcare Advocates learned for the first time that the Internet Archive web logs related to Defendants' conduct did, in fact, continue to exist. Id. Healthcare Advocates did not receive all of these web logs from Internet Archive until after the parties had reached terms of settlement at the end of August 2006, and did not have an opportunity to depose Internet Archive personnel until the end of September 2006. Id.



v.

Once the Internet Archive web logs related to Defendants' conduct was in hand, testifying computer forensic expert Gideon Lenkey finally was able to analyze and interpret both the Healthcare Advocates web logs side by side with the relevant Internet Archive web logs. Id. at ¶5. Despite HEFF's egregious spoliation of electronic evidence, Mr. Lenkey has been able, for the first time, to provide Healthcare Advocates with a report detailing the most complete understanding possible of the nature, extent and significance of Defendants' conduct so that Healthcare Advocates finally can conduct a meaningful assessment. Id. at Ex. D. Accordingly, Healthcare Advocates' cognizable CFAA damages include legal fees identifiable to its battle to secure Internet Archive web logs and the sworn testimony of Internet Archive personnel as well as the expenses of computer forensic experts Warren Kruse and Gideon Lenkey.

Cases cited by Defendants to support their view that Healthcare Advocates cannot meet the $5,000 threshold are inapposite, as the plaintiffs in those cases alleged losses that were far more tenuously related to the conduct of the defendants in those cases. For example, Defendants rely on Nexans Wires S.A. v. Sark-USA, Inc., 319 F.Supp.2d 468 (S.D.N.Y. 2004), asserting that Healthcare Advocates' losses are akin to the losses asserted by the plaintiff in Nexans Wires. However, in that case, the court found that the travel expenses of plaintiff's senior executives relating to a business trip to meet with their suppliers to discuss the business repercussions of an alleged CFAA violation were not "losses" pursuant to the CFAA. Nexans Wires, 319 F.Supp.2d at 476. In contrast, the losses sustained by Healthcare Advocates were directly linked to the unauthorized access; they were incurred by Healthcare Advocates to determine its legal obligations and corporate duties as a result of Defendants' conduct and to assess the nature, extent and degree of harm caused by Defendants' conduct.



v.

In sum, all of Healthcare Advocates' claimed losses were reasonably incurred responding to Defendants' conduct and gathering the information required to conduct a meaningful damage assessment. See SOF at ¶76. They aggregate to much more than the $5,000 statutory minimum and are fully reimbursable under the CFAA. There is no material dispute of fact concerning Healthcare Advocates' ability to satisfy this element of its CFAA claim.

## CONCLUSION

In view of the foregoing, summary judgment in favor of Defendants on the DMCA, copyright infringement and CFAA claims should be denied, and Healthcare Advocates is entitled to summary judgment on its DMCA and CFAA claims.

Dated: April 18, 2007

By: /s/ Scott S. Christie
Scott S. Christie, Esq.
Peter J. Boyer, Esq.
McCARTER & ENGLISH, LLP
Mellon Bank Center
1735 Market Street, Suite 700
Philadelphia, Pennsylvania 19103

*Attorneys for Plaintiff*
*Healthcare Advocates, Inc*