EXHIBIT 217

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

CHRISTOPHER SPECHT, JOHN GIBSON, MICHAEL FAGAN, and SEAN KELLY, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

NETSCAPE COMMUNICATIONS CORPORATION and AMERICA ONLINE, INC.

Defendants.

Civil Action No.
00 CIV. 4871 (AKH)

SHERRY WEINDORF, individually and on behalf of all others similarly situated,

Plaintiff,

v.

NETSCAPE COMMUNICATIONS CORPORATION and AMERICA ONLINE, INC.

Defendants.

Civil Action No.
00 CIV. 6219 (AKH)

MARK GRUBER, individually and on behalf of all others similarly situated,

Plaintiff,

v.

NETSCAPE COMMUNICATIONS CORPORATION and AMERICA ONLINE, INC.,

Defendants.

Civil Action No.
00 CIV. 6249 (AKH)

DEFENDANTS' MEMORANDUM
OF LAW IN SUPPORT OF MOTIONS TO DISMISS

Of Counsel:
David C. Goldberg
America Online, Inc.
22000 AOL Way
Dulles, Virginia 20166-9323

Janet Lee
Netscape Communications Corporation
501 East Middlefield Road, Bldg. 10
MS-MV002
Mountain View, California 94043

Patrick J. Carome (PC 7218)
Roger W. Yoerges (RY 6976)
Samir C. Jain (SJ 0409)
WILMER, CUTLER & PICKERING
2445 M Street, N.W.
Washington, DC 20037
Tel: 202-663-6000
Fax: 202-663-6363

Matthew P. Previn (MP 2173)
WILMER, CUTLER & PICKERING
399 Park Avenue
New York, New York 10022
Tel: 212-230-8800
Fax: 212-230-8888

Counsel for Defendants

Exhibit 217

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES **Page(s)**

Page(s)

CASES

STATUTES

MISCELLANEOUS

INTRODUCTION

Plaintiffs in these three related cases[1/] contend that a free software program that Netscape Communications Corporation ("Netscape") offered to assist Internet users in downloading files from the Internet operated unlawfully. With a heavy dose of alarmist rhetoric, Plaintiffs allege that Netscape and its parent company, America Online, Inc. ("AOL"), used this software — called SmartDownload — as a "bugging device" to "eavesdrop" on communications between the software's users and the Internet web sites from which they downloaded files, allegedly giving Defendants information that could be used to create "moment-by-moment profiles of file transactions" of Internet users and web site operators.

Whatever it is that Plaintiffs allege regarding the operation of SmartDownload, they fail to state a cause of action *as a matter of law*. Indeed, once one sifts through the rhetoric, Plaintiffs ultimately allege nothing more than that a now-superseded version of SmartDownload transmitted to Netscape's computer servers a few tidbits of information regarding certain types of file-download transactions — specifically, the electronic "address" of the file to be downloaded and codes that allegedly identified the user's computer. Plaintiffs do not allege that any human being at Netscape ever saw any of this information, do not identify any respect in which Netscape ever used any of this information for any purpose whatsoever, and do not claim that Netscape ever shared any of this information with any other person or entity. Not

---

1/ The three separate lawsuits that are the subject of this motion to dismiss have, as a formal matter, not been consolidated. Nonetheless, the proceedings to date in these three cases have been coordinated. The arguments for dismissal that Defendants are now asserting in the *Weindorf* and *Gruber* actions are identical, and all of those arguments also apply with full force to the *Specht* action. Accordingly, although Defendants are filing separate motions to dismiss in each of the three cases, they are submitting the same Memorandum of Law in support of each of the three motions to dismiss to avoid requiring the Court to review multiple duplicative papers.

surprisingly, therefore, Plaintiffs also fail to allege anything even to suggest that they have been economically injured by Netscape's software.

Based on these meager allegations, Plaintiffs claim, on behalf of themselves and one or more putative classes, that Netscape's distribution of this software violated two criminal statutes, the federal Wiretap Act (as amended by the Electronic Communications Privacy Act ("ECPA")), which prohibits certain "interceptions" of electronic communications, and the federal Computer Fraud and Abuse Act ("CFAA"), which was designed to prevent major criminal intrusions (or "hacking") into computer systems. Even accepting as true all of Plaintiffs' allegations (which Defendants must do for purposes of this motion), the facts alleged do not even begin to establish a violation of either of these statutes, both of which are highly technical in nature and were designed to address narrowly defined criminal conduct bearing no resemblance to what Plaintiffs allege.

While Defendants have a great many defenses to Plaintiffs' claims on both the facts and the law, Defendants' motions to dismiss focus on particularly obvious legal defects that mandate dismissal of all of the claims now. *First*, Plaintiffs' Wiretap Act claims fail at the threshold because, among other things, Plaintiffs do not (and cannot) allege that Netscape ever acquired data constituting the "*contents*" of any of their communications — even though acquisition of "contents" is the central prerequisite of an unlawful "interception" under the Wiretap Act. *Second*, Plaintiffs' CFAA claims fail at the threshold because they do not (and cannot) allege that they suffered economic damages of any sort, let alone economic damages in the amount of at least $5,000 per act, as the applicable statute expressly requires. As a result of these and other deficiencies, Plaintiffs' Complaints clearly fail to state a claim and must be dismissed.

BACKGROUND[2/]

Netscape and the SmartDownload Software

Defendant Netscape, now a wholly owned subsidiary of Defendant AOL, is a leading provider of Internet-related software, products, and services. (*See* Specht Amended Complaint ("Specht Am. Compl.") ¶¶ 10-11; Weindorf Complaint ("Weindorf Compl.") ¶¶ 8-9; Gruber Complaint ("Gruber Compl.") ¶¶ 8-9.) Netscape's flagship product is an Internet "browser" called "Navigator" (sometimes bundled with other Netscape software in a package called "Communicator") that allows users to locate, view, and interact with web sites that exist on the vast Internet. (*See* Specht Am. Compl. ¶ 10; Weindorf Compl. ¶ 8; Gruber Compl. ¶ 8.) A user can obtain Netscape's browser software at no charge by downloading it from Netscape's principal Internet web site, called Netcenter at the time of the Complaints, at www.netscape.com. (*See* Specht Am. Compl. ¶ 10.)

During the times relevant to the Complaints, Netscape also provided software known as SmartDownload, which consumers also could obtain through Netscape's web site free of charge.[3/] (*See* Specht Am. Compl. ¶¶ 24, 29.) SmartDownload could be used in conjunction with Netscape's browser software to help users download from the Internet to their personal computers certain types of electronic files — namely those containing an "exe" or "zip"

2/ Although Defendants do not concede the truth of the allegations contained in the Complaints, they must treat them as true for the limited purpose of this motion to dismiss. *See Patel v. Searles*, 305 F.3d 130, 134-35 (2d Cir. 2002).

3/ The version of SmartDownload that is the subject of the Complaints is the initial version, Version 1.1, that Netscape offered to the public during the period of November 1998 through early October 2000. (*Cf.* Specht Am. Compl. ¶ 24; Weindorf Compl. ¶ 22; Gruber Compl. ¶ 22.) All versions of SmartDownload that Netscape has distributed since early October 2000 lack the feature about which Plaintiffs complain. Unless otherwise specified, all references to SmartDownload in this memorandum are to Version 1.1.

extension.[4/] (Specht Am. Compl. ¶¶ 8, 25; Weindorf Compl. ¶ 23; Gruber Compl. ¶¶ 7, 23.) Among other things, the SmartDownload software was designed to allow a user to pause and resume downloads midstream and to resume downloads that were interrupted because of a lost Internet connection. (*See* Specht Am. Compl. ¶ 25; Weindorf Compl. ¶ 23; Gruber Compl. ¶ 23.) One of Netscape's principal motivations for offering SmartDownload was to ease the difficulties consumers faced in obtaining Netscape's browser software, which Netscape (unlike its principal competitor, Microsoft, whose browser software generally came pre-installed on users' computers) had to distribute mainly through Internet downloads. (*See* Specht Am. Compl. ¶¶ 26-28; Weindorf Compl. ¶¶ 24-26; Gruber Compl. ¶¶ 24-26.)

According to the Complaints, when SmartDownload was invoked to facilitate the download of an electronic file from an Internet web site, it also transmitted to Netscape certain information. In particular, SmartDownload allegedly sent a string of data that contained the "name and Internet address of the file and the Web site from which it [was] being sent" and a "key," which consisted of "the name of [the user's] computer, and the serial number of the primary storage volume." (Specht Am. Compl. ¶¶ 33, 35; Weindorf Compl. ¶¶ 31, 33; Gruber Compl. ¶¶ 31, 33.) Plaintiffs do not and cannot allege that this "key" could be used by Netscape to identify an actual person. Nor do they allege that anyone at Netscape ever actually saw or accessed any of this data, that Netscape ever made any use of this data, or that Netscape ever disclosed any of this information to any third party. Moreover, they do not allege that Netscape

---

[4/] Files with "exe" extensions are called "executable files," which are generally "computer program[s] that [are] ready to run," such as application programs like spreadsheets and word processors. Newton's Telecom Dictionary 279 (18th ed. 2002). Files with "zip" extensions have been compressed to facilitate more rapid transmission over the Internet or telephone lines. *See id.* at 846 (describing "zip" files).

ever received the contents of any file that any user of SmartDownload obtained using the software.

Plaintiffs further allege that, like "[m]any different Web sites," the Netscape browser software "creates and stores on the Web user's computer a small text file known as a 'cookie'" and that this cookie "contains a unique and unchanging string of characters that is different from the string placed by Communicator in any other cookie on any other computer." (Specht Am. Compl. ¶¶ 30-31; Weindorf Compl. ¶¶ 28-29; Gruber Compl. ¶¶ 28-29) The Complaints further note that cookies may be used to "provide temporary identification for purposes such as electronic commerce " (Specht Am. Compl. ¶ 31; Weindorf Compl. ¶ 29; Gruber Compl. ¶ 29.) According to the Complaint, the SmartDownload software also sent to Netscape the "cookie" created by Communicator (Specht Am. Compl. ¶¶ 35-36; Weindorf Compl ¶¶ 33-34; Gruber Compl. ¶¶ 33-34)

Plaintiffs

This litigation began when Plaintiff Christopher Specht, suing on his own, filed a putative class action Complaint (No 00 Civ. 4871) against Netscape and AOL in June 2000. Before that complaint was served, it was superseded by an Amended Complaint, in which Specht was joined by three additional plaintiffs (John Gibson, Michael Fagan, and Sean Kelly) Soon thereafter, Plaintiffs Sherry Weindorf and Mark Gruber each filed separate putative class action Complaints (Nos. 00 Civ. 6219 and 00 Civ 6249) that, except for the allegations identifying the Plaintiffs, were essentially cookie-cutter reiterations of the Amended Complaint in the *Specht* case

Five of the six named Plaintiffs — Gibson, Fagan, Kelly, Weindort, and Gruber (the "User Plaintiffs") — are individuals who allegedly obtained the SmartDownload software and used it to help download files from Web sites on the Internet. (*See* Specht Am Compl. ¶ 9;

Weindorf Compl. ¶ 7; Gruber Compl. ¶ 7.) The Complaints do not contain any allegations concerning the types of files the User Plaintiffs allegedly obtained using SmartDownload or the frequency with which they used the software.

In contrast, Plaintiff Specht does not claim to have used the SmartDownload software at all. Rather, the Amended Complaint in the *Specht* action alleges that he "maintains Web sites on the Internet at which visitors are invited to download exe files." (Specht Am. Compl. ¶ 7.) The only files that Specht alleges he offered for download from his web sites are "exe files that can be used to connect to — and to open accounts with — small Internet Service Providers." (*Id.* ¶ 37.) The Amended Complaint does not allege that anyone ever used SmartDownload software to download any such file from any web site maintained by Specht.

Plaintiffs' Claims

Each of the Complaints asserts two claims under federal criminal statutes. First, Plaintiffs claim that Netscape and AOL violated the Wiretap Act, 18 U.S.C. §§ 2510 *et seq.*, as amended by ECPA, because the SmartDownload software allegedly "intercepted" Plaintiffs' communications by obtaining the "file name, its source, and the Internet identities of the participants" relating to such communications. (Specht Am. Compl. ¶¶ 46-50; Weindorf Compl. ¶¶ 44-48; Gruber Compl. ¶¶ 44-48.) Second, Plaintiffs claim that Netscape and AOL violated the CFAA, 18 U.S.C. § 1030, because, by allegedly "using SmartDownload to secretly obtain information contained in the computers of SmartDownload users about what files are downloaded," they allegedly "accesse[d] a computer without authorization or exceed[ed] authorized access." (Specht Am. Compl. ¶ 59; Weindorf Compl. ¶ 57; Gruber Compl. ¶ 57.) The Complaints do not allege that any of the Plaintiffs suffered any economic damage as a result of any of these alleged violations.

Procedural History

Shortly after the Complaints were filed, Defendants moved to compel arbitration and stay proceedings on the ground that the license agreements associated with the SmartDownload software and the browser software required Plaintiffs to pursue their claims through arbitration. This Court denied Defendants' motion, *see* 150 F Supp 2d 585 (S D N Y 2001), and the Second Circuit affirmed on interlocutory appeal, *see* 306 F 3d 17 (2d Cir 2002). Netscape and AOL now move to dismiss all of Plaintiffs' claims on the merits because they fail to state a claim as a matter of law.

ARGUMENT

I. PLAINTIFFS' WIRETAP ACT CLAIMS FAIL AT THE THRESHOLD.

Plaintiffs have failed to allege critical elements necessary to establish that they were victims of an unlawful "interception" within the meaning of the Wiretap Act, 18 U S C. §§ 2510 *et seq*. An "interception" occurs under the Wiretap Act only if a person acquires the "*contents*" of a communication, not other information associated with a communication. None of the information that Plaintiffs claim the SmartDownload software transmitted to Netscape, however, constitutes the "contents" of a communication within the meaning of the Wiretap Act, and all of the Plaintiffs' Wiretap Act claims therefore fail as a matter of law Moreover, Plaintiff Specht (who does not claim ever to have used Netscape's software) also fails to state a claim under the Wiretap Act for two additional reasons: (1) he has failed to allege that anyone using SmartDownload ever obtained any file from any of his web sites, which means *a fortiori* that he has not alleged that he has been a victim of any unlawful interception; and (2) even if he were able to cure that defect, he still has not alleged, and cannot allege, that his *own* communication

(in contrast to the communication of a SmartDownload user) was the subject of an alleged interception, as is essential for a private cause of action under the Wiretap Act.

A. Plaintiffs' Wiretap Act Claims Fail Because They Have Failed to Allege That Defendants "Intercept[ed]" the "Contents" of an Electronic Communication Within the Meaning of the Wiretap Act.

Plaintiffs' claims rely on section 2511 of the Wiretap Act, a criminal statute that makes it unlawful to "intentionally *intercept*[]" an electronic communication or to "intentionally use[] . . . *the contents* of any . . . electronic communication, knowing or having reason to know that the information was obtained through [an] *interception* . . . in violation of this subsection." 18 U.S.C. § 2511(1)(a), (d) (2002) (emphasis added).[5/] The statute in turn defines the term "intercept" to mean "the aural or other acquisition of the *contents* of any wire, electronic, or oral communication." *See* 18 U.S.C. § 2510(4) (2002) (emphasis added); *see also United States v. New York Tel. Co.*, 434 U.S. 159, 167 (1977) ("Pen registers [which collect telephone numbers dialed] do not 'intercept' because they do not acquire the 'contents' of communications . . . ."). The Wiretap Act defines "contents" to include only "information concerning the *substance, purport, or meaning* of that communication." 18 U.S.C. § 2510(8) (2002) (emphasis added). Therefore, a party does not violate the Wiretap Act's prohibition against "intercepting" a communication (or using the fruits of such an "interception") unless the information acquired is "contents" — that is, information that concerns "the substance, purport, or meaning" of that

---

[5/] Each of the Complaints alleges in a single, conclusory paragraph that Defendants also "use[d]" the contents of their electronic communications. (Specht Am. Compl. ¶ 50; Weindorf Compl. ¶ 48; Gruber Compl. ¶ 48.) But the Complaints do not contain any allegations as to how Netscape purportedly "used" any information it received. Thus, Plaintiffs' baldly conclusory assertion that Netscape somehow violated the Wiretap Act's prohibition on "use" of the "contents" of an intercepted communication fails to state a claim for this additional reason. *See, e.g., Jones v. Ocwen Fed. Bank*, 147 F. Supp. 2d 219, 224 (S.D.N.Y. 2001) ("baldly conclusory" complaint is inadequately pleaded); *Shuster v. Oppelman*, 962 F. Supp. 394, 395 (S.D.N.Y. 1997) (same).

communication By contrast, transactional information about a communication does not fall within the category of "contents."

Plaintiffs claim that certain information that was allegedly sent to Netscape whenever a SmartDownload user downloaded a file from an Internet web site — namely the "file name, its source, and the Internet identities of the participants" — was a part of the "contents" of an electronic communication between the user and the web site. (Specht Am. Compl. ¶ 47; Weindorf Compl. ¶ 45; Gruber Compl. ¶ 45.) But the law is clear that these kinds of data are not part of the "contents."[6/]

First, the "identities of the participants" in an electronic communication unquestionably are not part of that communication's contents. Indeed, although the original definition of "contents" in the Wiretap Act expressly included the "identities of the parties," Congress expressly *deleted* parties' identities from the statutory definition when it amended the Wiretap Act by enacting the ECPA in 1986 As the pertinent Senate Report explained, "[s]ubsection 101(a)(5) of the Electronic Communications Privacy Act amends current section 2510(8) of title 18 *to exclude from the definition of the term 'contents,' the identity of the parties or the existence of the communication*. It thus distinguishes between the substance, purport or meaning of the communication and the existence of the communication or transactional records about it." *See* S.

6/ Moreover, the Court must construe the Wiretap Act's definition of "contents" strictly, because that construction would likewise apply in criminal cases brought under the Act *See Simpson v. Simpson*, 490 F.2d 803, 809 (5th Cir. 1974) (holding that a court construing the Wiretap Act in a civil suit is "bound by the principle that criminal statutes must be strictly construed, to avoid ensnaring behavior that is not clearly proscribed," because the Act has "the primary goal of controlling crime" and "also prescribes criminal sanctions for its violators"); *see also FCC v. American Broad. Co.*, 347 U S 284, 296 (1954) (holding that "the well-established principle that penal statutes are to be construed strictly" applies in a civil case where "the same construction would likewise apply in criminal cases"); *Schwartz v. Romnes*, 495 F 2d 844, 848-49 (2d Cir. 1974) (holding, in a civil case, that the penal statute at issue must be strictly construed).

Rep. No. 99-541, at 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3567 (emphasis added); *see also* H.R. Rep. No. 99-647, at 34 (1986) ("This amendment also makes clear the distinction between contents of communications and transactional records."). In view of this amendment to the Wiretap Act's definition of "contents," Plaintiffs' allegation that Netscape acquired the "contents" of a communication because SmartDownload allegedly transmitted to Netscape the "identities of the participants" is clearly wrong as a matter of law.

Second, the only other information allegedly transmitted to Netscape — "the name and Internet address of the file and the Web site from which it is being sent" (Specht Am. Compl. ¶ 35; Weindorf Compl. ¶ 33; Gruber Compl. ¶ 33) — is also not "contents" under the Wiretap Act. Plaintiffs' allegation on this point is simply a somewhat redundant way of contending that SmartDownload sent to Netscape the Internet address, also known as Uniform Resource Locator ("URL"), for the file that a user was about to download. A URL is merely the code that identifies the address on the Internet where a particular file or other source of electronic information is located.[7/]

As numerous courts have recognized, a URL "functions much like a telephone number." *Sallen v. Corinthians Licenciamentos LTDA*, 273 F.3d 14, 19 (1st Cir. 2001); *see also Reno v. ACLU*, 521 U.S. 844, 852 (1997) ("Each [web page] has its own address – 'rather like a telephone number.'"); *Image Online Design, Inc. v. Core Ass'n*, 120 F. Supp. 2d 870 (C.D. Cal. 2000) (equating telephone numbers and URL addresses). URLs are simply a means of establishing communication that allows one party to find another party or other source of

---

7/ *See, e.g.*, Newton's Telecom Dictionary 785 (18th ed. 2002) ("A URL is a fancy name for an Internet address."); Miriam-Webster's Collegiate Dictionary 1296 (10th ed. 2001) (defining URL as "the address of a computer or a document on the Internet that consists of a communications protocol followed by a colon and two slashes (as http://), the identifier of a computer (as www.m-w.com) and usually a path through a directory to a file").

information with which to communicate *See, e.g., ACTV, Inc. v. Walt Disney Co*, 204 F. Supp. 2d 691, 692 (S.D.N.Y. 2002) (describing URLs as "complete site addresses, specifying both protocol type and resource location, that enable one to access sites throughout the Internet"). Much like the role that a telephone number serves in the telephone network, a URL specifies the network location of the destination — whether a phone or a computer server — that the user is trying to reach. The Supreme Court has held that such "means of establishing communication" are not "contents" for purposes of the Wiretap Act. *New York Tel. Co.*, 434 U.S. at 166-67 (holding that telephone numbers do not constitute "contents" as defined by 18 U.S.C. § 2510(8)); *see also Smith v. Maryland*, 442 U.S. 735, 741 (1979) (holding that telephone numbers are not contents of communications). Indeed, at least one court has specifically held that the URLs of web sites accessed by a user are not "contents" of a communication. *See United States v. Allen*, 53 M.J. 402, 409 (C.A.A.F. 2000) (concluding that "a log identifying the date, time, user, and *detailed internet address of sites accessed*" by a user constituted "a record or other information pertaining to a subscriber or customer of such service" and not "contents") (emphasis added).

More generally, in amending the Wiretap Act with the ECPA, Congress "distinguishe[d] between the substance, purport or meaning of the communication and the existence of the communication or *transactional records* about it." S. Rep. No. 99-541, at 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3567 (emphasis added); *see also* H.R. Rep. No. 99-647, at 34 (1986) (the amendment "makes clear the distinction between contents of communications and *transactional records*") (emphasis added). The URL address of a file downloaded by an Internet user is nothing more than part of a "transactional record" concerning the electronic communication, just as a log of telephone numbers dialed is a transactional record of wire communications. Several courts have made clear that even detailed transactional information

concerning specific communications does not amount to the "contents" or "substance, purport or meaning" of those communications. *See, e.g.*, *In re United States*, 36 F. Supp. 2d 430, 432 (D. Mass. 1999) (holding that legal requirements under the ECPA differ depending on whether the information at issue is the "*contents* of electronic communications or merely records related to them (i.e., personal information of subscribers, *user activity logs*, billing records and so on)") (emphasis added); *Hill v. MCI WorldCom Communications, Inc.*, 120 F. Supp. 2d 1194, 1195-96 (S.D. Iowa 2000) (holding that "invoice/billing information and the names, addresses, and phone numbers of parties" called by the plaintiffs did not constitute "contents" under the ECPA); *see also Gilday v. Dubois*, 124 F.3d 277, 296 n.27 (1st Cir. 1997) (holding that call "detailing" does not intercept the "contents" of communications under the Wiretap Act because it "simply captures electronic signals relating to the PIN of the caller, the number called, and the date, time and length of the call").[8/]

[8/] The structure of the Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.*, which was enacted as part of the ECPA and utilizes the Wiretap Act's definition of "contents," confirms that there is a fundamental distinction between transactional records concerning a communication (such as a URL for a file to be downloaded) and the actual contents of a communication (such as the material contained in such a file). Specifically, the Stored Communications Act establishes different levels of official process that a governmental entity must use to obtain different kinds of subscriber information from an electronic service provider. To obtain the "contents" of a stored electronic communication, the government generally must use a criminal search warrant. 18 U.S.C. § 2703(a), (b). In contrast, the government may use a less burdensome court order to obtain any type of subscriber information *other than contents*, *id.* § 2703(c), and may even use a simple subpoena to obtain certain specified types of basic non-content information, namely a customer's name, address, "local and long distance telephone connection records, or records of session times and durations," "length of service (including start date) and types of service utilized," "telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address," and "means and source of payment for such service (including any credit card or bank account number)." *Id.* § 2703(c)(2). These provisions make clear that there are vast categories of information that pertain to an individual's electronic communications but that do not qualify as the "contents" of those communications. The URL of a file to be downloaded plainly falls within one of these non-contents categories.

That the acquisition of the Internet address of an electronic file that a computer user is about to download from an Internet web site does not constitute an interception of the "contents" of a communication between the user and the site is entirely sensible. This situation is not materially different from one in which a telephone user, wishing to hear a recorded voice message that he or she believes to be available at the end of a particular telephone line (for example, a "1-900" toll number where a recorded message is played for a fee), dials the telephone number to establish a connection to the recording device that will play that message. If either the telephone company providing the user's telephone service or a law enforcement agency using a pen register or similar device acquired the particular telephone number that the caller dialed, there would be no doubt under well-established authorities that the "contents" of the caller's communication had not been acquired *See, e.g.*, *New York Tel. Co.*, 434 U.S. at 166-67 (holding that telephone numbers are not contents of communications); *Hill*, 120 F. Supp. 2d at 1195-96 (holding that "names, addresses, and phone numbers of parties" called by the plaintiffs did not constitute "contents" of communications). And this would be true even though anyone possessing that phone number could dial the number, listen to the recording himself, and surmise that the recording he hears is probably what the original caller had heard For the same reasons, the URLs of Internet web sites that SmartDownload allegedly transmitted to Netscape did not constitute the "contents" of the underlying communications. Again, this would be true even though it might have been theoretically possible (though nothing of the sort is alleged here) for someone at Netscape to have plugged one of those URL addresses into his own Internet browser, obtained for himself the contents of the electronic file then stored at that address, and on that basis have made an educated guess that some unknown person using SmartDownload had probably obtained the very same contents at an earlier time.

The most basic prerequisite of an "interception" under the Wiretap Act is the acquisition of the actual "contents" of a communication. Under the facts as alleged in the Complaints, however, the information allegedly transmitted to Netscape by the SmartDownload software was not part of the "contents" of Plaintiffs' communications with a third party as a matter of law, and Plaintiffs' Wiretap Act claims must be dismissed.

B. Specht's Wiretap Act Claim Must Also Be Dismissed Because He Does Not Allege That He Was a Party to Any Supposedly Intercepted Communication.

Plaintiff Specht's Wiretap Act claim also fails for the independent reason that his Amended Complaint does not allege that he was ever a party to any communication that allegedly was intercepted by the operation of the SmartDownload software. Specht alleges, on behalf of himself and a putative class of web site operators whom he purports to represent, that he "maintains Web sites on the Internet at which visitors are invited to download exe files." (Specht Am. Compl. ¶ 7; *see also id.* ¶ 37 ("[P]laintiff Specht offers visitors to his Web sites the opportunity to download exe files that can be used to connect to — and to open accounts with — small Internet service providers that compete directly with defendant AOL.").) His Complaint, however, contains *no* allegation that any person ever used SmartDownload to obtain a file from any of his web sites, or that any person who did so was not aware of (and therefore did not consent to) SmartDownload's communication of certain information to Netscape.[9/] Thus, even assuming the truth of Specht's allegations and assuming (contrary to the foregoing argument) that SmartDownload did intercept the communications of users who used it to download files, the Complaint lacks any averment that any communication to which Specht was a party was, in

---

9/ Under the Wiretap Act, if *either* party to a communication consents to an alleged interception, that interception is not a violation of the statute. 18 U.S.C. § 2511(2)(d).

fact, unlawfully intercepted by the operation of the SmartDownload software. As a result, Specht has failed — at the most basic level — to state any claim under the Wiretap Act.

C. Specht's Wiretap Act Claim Also Fails Because He Does Not Allege That *His Own* Communications Were Intercepted Within the Meaning of the Statute.

Under 18 U.S.C. § 2520(a), which confers on private parties a cause of action for certain Wiretap Act violations, only a person "whose wire, oral, or electronic communication is intercepted" may file suit. Because Plaintiff Specht does not allege that *his own* communication was intercepted within the meaning of that provision, his Wiretap Act argument fails to state a claim and should be dismissed.

As discussed above, Specht alleges that he maintained one or more public Internet web sites from which any Internet user, including any user of SmartDownload, could have downloaded certain "exe files." (*See* Specht Am. Compl. ¶¶ 7, 37.) He further alleges that SmartDownload software residing on a user's computer caused information to be transferred from the user's computer to Netscape "each time a Web user downloads any file from *any* site on the Internet using SmartDownload." *Id.* ¶ 35 (emphasis in original). Specht does not allege, however, that SmartDownload software causes any information to be sent to Netscape when a web site responds to a user's electronic communication requesting a download, or when a user receives any such response.

Taking Specht's allegations as true, then, the putative "interception" that SmartDownload software supposedly effects is of a "communication" *by the software user* to the web site, not of any communication by the web site back to the user. In other words, if any SmartDownload user ever downloaded a file from Specht's web site, the communication that was allegedly intercepted was the *user's communication* to the Specht web site containing the electronic address of the file to be downloaded, not any response that the Specht web site would have made to that request.

Thus, any communication that was allegedly intercepted necessarily would have been the user's communication, not Specht's. This distinction reveals yet another fatal defect in Specht's claim under the Wiretap Act.

The Wiretap Act provides a private cause of action only to the person who initiates a "communication" that has been "intercepted," not to someone who merely is the intended recipient of that communication. This conclusion stems directly from the very words of the provision of the Wiretap Act that creates a civil action, section 2520(a), which states that only a person "whose . . . communication" is intercepted may sue for relief. This conclusion is also confirmed by the fact that *another* section of the Wiretap Act permits a broader class of individuals to seek suppression of unlawfully intercepted communications in a criminal trial. Specifically, section 2518 of the statute permits any "aggrieved person" to move to suppress an unlawfully intercepted message, *see id.* § 2518(10)(a), and an "aggrieved person" is defined to include any "party to . . . [a] communication that was" intercepted, *see id.* § 2510(11). Under well-accepted canons of statutory construction, the existence of this parallel — and broader — language in another section of the Wiretap Act means that the class of parties that can bring a civil claim under section 2520(a) must be read narrowly. *See United States v. Maria*, 186 F.3d 65, 71 (2d Cir. 1999) ("As a general matter, the use of different words within the same statutory context strongly suggests that different meanings were intended."). The only reasonable way to give these differing statutory terms distinct meanings is to interpret "whose . . . communication" to refer only to the initiator of a communication and to interpret "party to . . . [a] communication" as referring to both the initiator and the recipient(s).

Because Specht has not alleged that any "communication" that he initiated was "intercepted" within the meaning of 18 U.S.C. § 2520(a), and because he was at most a recipient

party to an allegedly intercepted communication, he cannot claim that his own communication has been "intercepted" within the meaning of 18 U.S.C. § 2520(a). For this reason as well, his Wiretap Act claim is fatally deficient as a matter of law and must be dismissed.

II. PLAINTIFFS HAVE FAILED TO ALLEGE AN ACTIONABLE VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT.

Under the version of the CFAA that governs these actions,[10/] a plaintiff can maintain a cause of action only if he alleges that he has suffered "damage or loss" totaling at least $5,000, and that the claimed "damage or loss" consists of "economic damages."[11/] *See* 18 U.S.C. §§ 1030(e)(8), (g) (2001) (providing that "[d]amages for violations involving damage as defined in [18 U.S.C. § 1030](e)(8)(A) are limited to economic damages" and that such damages must be "at least $5000") (subsequently amended, Oct. 2001). On this point, the Plaintiffs have alleged nothing more than that "[b]y using SmartDownload to secretly obtain information contained in the computers of [Internet users] about what files are downloaded, each defendant has caused

---

10/ In October 2001 — well after the matters alleged in Plaintiffs' Complaints are alleged to have occurred and after the Complaints were filed — amendments to certain sections of the CFAA, including the standards for bringing civil actions under 18 U.S.C. § 1030, were enacted into law. To the extent that those amendments may have expanded the scope of civil CFAA liability, however, Plaintiffs cannot take advantage of those amendments retroactively. *See Organizacion JD LIDA v. U.S. Dep't of Justice*, 124 F.3d 354, 358 (2d Cir. 1997) (refusing to apply amended ECPA to conduct that occurred before the amendment because "application of the amended ECPA . . . would subject defendants to increased liability for acts that antedate the effective date of the amendment" and would "*create*[] jurisdiction where none previously existed"); *see also Landgraf v. USI Film Prods.*, 511 U.S. 244, 265 (1994) (holding that courts must refuse retroactive application of statutes if such application would "increase a party's liability for past conduct," unless Congress has clearly expressed its intent to allow such application to occur).

11/ Under the pre-amendment version of 18 U.S.C. § 1030(g), the $5,000 "damage or loss" threshold does not apply to CFAA violations that impair medical records, cause physical injury to any person, or threaten public safety. *See* 18 U.S.C. §§ 1030(e)(8)(B) - (D) (2001) (subsequently amended, Oct. 2001); *see also In re Intuit Privacy Litig.*, 138 F. Supp. 2d 1272, 1281 (C.D. Cal. 2001). Those exceptions are clearly inapplicable here.

'damage' within the meaning of § 1030." (Specht Am. Compl. ¶ 60; Weindorf Compl. ¶ 58; Gruber Compl. ¶ 58.) This conclusory allegation plainly cannot sustain their CFAA claims, however, because none of the Plaintiffs makes *any* allegation that he or she has suffered *any* economic damages, much less economic damages amounting to at least $5,000.

As this Court has previously held, a plaintiff's failure to plead that he or she has suffered "economic damage" is itself sufficient to require dismissal of a CFAA claim. *See Letscher v. Swiss Bank Corp.*, No. 94 Civ. 8277 (LBS), 1996 WL 183019, at *3 (S.D.N.Y. Apr. 16, 1996) (Sand, J.) (dismissing CFAA claim because plaintiff failed to allege that he suffered economic damage); *see also In re Intuit Privacy Litig.*, 138 F. Supp. 2d 1272, 1281 & n.17 (C.D. Cal. 2001) (granting defendant's motion to dismiss for failure to state a claim where plaintiffs made no allegation of economic damages, and finding that the complaint "does not include sufficient facts constituting an allegation or reasonable inference therefrom that Plaintiffs suffered at least $5,000 in economic damages").

Indeed, given that the Complaints do not (and cannot) allege any facts showing that Netscape ever used or disclosed any of the information that SmartDownload allegedly transmitted to Netscape, there is no reason to believe that any Plaintiff could plead economic damages of any kind. *See In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 525-26 (S.D.N.Y. 2001) (Buchwald, J.) (rejecting plaintiffs' claims that the value of either defendant's "opportunity to present plaintiffs with advertising" or plaintiffs' demographic information could be considered a measure of plaintiffs' economic damages). Because Plaintiffs have not pled that they suffered economic damages, their CFAA arguments fail to state a claim and must be dismissed. *See id.* at 524 n.33 (noting that CFAA claims alleging injury in the form of emotional

distress based on invasion of privacy, trespass, and misappropriation of confidential data are "not actionable because only economic losses are recoverable under § 1030(g)").

Plaintiffs' CFAA claims also fail at the threshold because not one of the Plaintiffs has alleged that he or she suffered "at least $5,000" in economic damage. 18 U.S.C. § 1030(e)(8) (2001 ed.); *see In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d at 520-23. Critically, to satisfy this $5,000 "damage or loss" criterion, a plaintiff must point to *individual acts* by the defendant that caused at least $5,000 in economic injury, as opposed to a series of acts resulting in aggregated damages of $5,000 or more. *Id.* at 523 (damages may only be aggregated "for a single act"). In other words, a plaintiff must be able to point to a single time when Netscape allegedly accessed his or her computer without authorization that resulted in $5,000 in economic damage. As this Court explained, this interpretation reflects congressional intent to limit the CFAA to major crimes. *See id.* at 524. Moreover, this Court has made clear that "the definition of a prohibited act turns on the [defendant's] access to a *particular* computer." *See id.* at 524 (emphasis in original); *Chance v. Avenue A, Inc.*, 165 F. Supp. 2d 1153, 1159 (W.D. Wash. 2001) (each discrete communication between the defendant's computer and the plaintiff's computer constitutes a singular act for which at least $5,000 of damages must be established).

To have a viable claim, each Plaintiff is required to allege "damage or loss" amounting to $5,000 to him or her individually resulting from a single unauthorized access to his or her computer. Here, none of the Plaintiffs has pled *any* economic damage, let alone $5,000 in

economic damage as a result of a single act of unauthorized access by Netscape. Their CFAA claims accordingly must be dismissed.[12/]

CONCLUSION

For the foregoing reasons, the Court should grant Defendants Netscape's and AOL's motions and dismiss each of Plaintiffs' claims with prejudice.

Dated: January 15, 2003

Respectfully submitted,

By: Patrick J. Carome /rvl

Patrick J. Carome (PC 7218)
Roger W. Yoerges (RY 6976)
Samir C. Jain (SJ 0409)
WILMER, CUTLER & PICKERING
2445 M Street, N.W.
Washington, D.C. 20037
Tel: 202-663-6000
Fax: 202-663-6363

Matthew P. Previn (MP 2173)
WILMER, CUTLER & PICKERING
399 Park Avenue
New York, New York 10022
Tel: 212-230-8800
Fax: 212-230-8888

Counsel for Defendants

Of Counsel
David C. Goldberg
America Online, Inc.
22000 AOL Way
Dulles, Virginia 20166-9323

Janet Lee
Netscape Communications Corporation
501 East Middlefield Road, Bldg. 10
MS-MV002
Mountain View, California 94043

12/ As with his Wiretap Act claim, Plaintiff Specht's CFAA claim is also fraught with additional fatal defects, including most obviously the fact that (as described in Section I.B.) he has failed to allege that there was ever an occasion when anyone using SmartDownload accessed his web site.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

CHRISTOPHER SPECHT, JOHN GIBSON, MICHAEL FAGAN, and SEAN KELLY, individually and on behalf of all those similarly situated,

Plaintiffs,

v.

NETSCAPE COMMUNICATIONS CORPORATION and AMERICA ONLINE, INC.,

Defendants.

Civil Action No.
00 CIV 4871 (AKH)

SHERRY WEINDORF, individually and on behalf of all those similarly situated,

Plaintiff,

v.

NETSCAPE COMMUNICATIONS CORPORATION and AMERICA ONLINE, INC.,

Defendants.

Civil Action No.
00 CIV 6219 (AKH)

MARK GRUBER, individually and on behalf of all those similarly situated,

Plaintiff,

v.

NETSCAPE COMMUNICATIONS CORPORATION and AMERICA ONLINE, INC.,

Defendants.

Civil Action No.
00 CIV 6249 (AKH)

AFFIDAVIT OF SERVICE

STATE OF NEW YORK)
:ss.:
COUNTY OF NEW YORK)

KIYEONG LEE, being duly sworn, deposes and says:

1. I am over 18 years of age and am employed by Wilmer, Cutler & Pickering and am not a party to this action.

2. On January 15, 2003, I caused a true and correct copy of the attached **Defendants' Memorandum Of Law In Support Of Motions To Dismiss** to be served by hand on the following parties:

Joshua N. Rubin, Esq.
Abbey, Gardy & Squitieri, LLP
212 East 39th St.
New York, NY 10016

James V. Bashian, Esq.
Oren S. Gishkan, Esq.
Law Offices of James V. Bashian
500 Fifth Avenue
Suite 2800
New York, NY 10010

and by FedEx, next business day delivery, on the following party:

George G. Mahfood, Esq.
Leesfield, Leighton, Rubio & Mahfood
2350 South Dixie Highway
Miami, FL 33133

Kiyeong Lee

Sworn to before me this
15th day of January, 2003

Notary Public

DANIEL J. BRUNO
Notary Public, State Of New York
No. 01BR6054536
Qualified In Kings County
Commission Expires Feb. 05, 2003