EXHIBIT 226

3/4/03

#92

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)

PLAINTIFFS' AMENDED MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANTS' MOTIONS TO DISMISS

Ex 226

Exhibit 226

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

INTRODUCTION 2

ARGUMENT 5

I. SmartDownload Transmitted the "Contents" of Electronic Communications 8

II. Mr. Specht was a Party to Intercepted Communications. 11

III. Mr. Specht Has Standing 12

IV. CFAA Claims May be Aggregated. 17

CONCLUSION 22

TABLE OF AUTHORITIES

CASES

Conley v. Gibson,
355 U.S. 41 (1957). 7, 13

British Telecom. PLC v. Prodigy Comm. Corp.,
217 F. Supp. 2d 399 (S.D.N.Y. 2002) 13

Fischer v. Mt. Olive Lutheran Church, Inc.,
207 F. Supp. 2d 914 (W.D. Wis. 2002) 14, 16

Fraser v. Nationwide Mut. Ins. Co.,
135 F. Supp. 2d 623 (E.D. Pa. 2001) 14, 16

Hishon v. King & Spaulding,
467 U.S. 69 (1984) 6

In re AOL, Inc. Version 5.0 Software Litig.,
168 F. Supp. 2d 1359 (S.D. Fla. 2001) 18, 21

In re Doubleclick Inc. Privacy Litig.,
154 F. Supp. 2d 497 (S.D.N.Y. 2001) 18, 21

In re Toys R Us, Inc. Privacy Litig.,
MDL Nos. M-00-1381 MMC, C-00-2746 MMC,
2001 U.S. Dist. Lexis 16947 (N.D. Ca. Oct. 9, 2001) 18, 20-21

Ingenix, Inc. v. Claude LaGalante,
No 02-876, 2002 U.S. Dist. Lexis 5795 (E.D. La. March 28, 2002) 18

In re Intuit Privacy Litig.,
138 F. Supp. 2d 1272 (C.D. Ca. 2001) 19, 21

Patel v. Searles,
305 F.3d 130 (2d Cir. 2002) 6

United States, v. Allen,
53 M.J. 402 (C.A.A.F. 2000) 10

United States v. Morris,
928 F.2d 504 (2d Cir. 1991) 19

Water-Works Co. v. Barret,
103 U.S. 516 (1881) 12

STATUTES

Computer Fraud and Abuse Act:

18 U.S.C. § 1030(e)(8) 17
18 U.S.C. § 1030(e)(8)(A) 17, 18, 20
18 U.S.C. § 1030(a)(5)(A) 17

Electronic Communications Privacy Act:

18 U.S.C. § 2510(11) 16
18 U.S.C. § 2510(12) 14
18 U.S.C. § 2511 ..... 16, 17
18 U.S.C. § 2511(1) 11
18 U.S.C. § 2511(2)(d) 15
18 U.S.C. § 2511(2)(h) 9
18 U.S.C. § 2518 17
18 U.S.C. § 2520 ..... 16, 17
18 U.S.C. § 2520(a) 11, 12, 13

Federal Rules of Civil Procedure:

Rule 8 ..... 6, 13

LEGISLATIVE HISTORY

S. Rep. No. 99-541 (1986),
reprinted in 1986 U.S.C.C.A.N. 3555 ..... 7, 15, 16, 17

146 Cong.Rec. E1949-04, 2000 WL 1598743 (Cong. Rec.)
(106th Cong. Oct. 26, 2000) 5

147 Cong. Rec. S636-04, 2001 WL 69660 (Cong. Rec.)
(107th Cong. Jan. 29, 2001); 5

PLAINTIFFS' AMENDED MEMORANDUM OF LAW IN OPPOSITIION TO DEFENDANTS' MOTIONS TO DISMISS

Plaintiffs, by their undersigned counsel, respectfully submit this Amended Memorandum of Law in Opposition to Defendants' Motions to Dismiss.

INTRODUCTION

We live in a country that has historically protected our personal privacy. We have always believed that people should be free from intrusion by commercial and governmental interests that might otherwise profit from a license to insert their eyes or ears into our private business. We abhor surveillance on principle and we have embodied that principle in laws, including those asserted herein, that protect us from surveillance except where there is a strong public interest at stake.

There is no public interest at all supporting the surveillance complained of in this case. The only interest at stake in this case is the desire of a large, powerful media company to secretly obtain information about people, including sensitive personal information, to use, trade, or sell.

Plaintiffs' claim is that Defendants used their SmartDownload software to violate the Electronic Communications Privacy Act (the "ECPA") and the Computer Fraud and Abuse Act (the "CFAA") by intercepting Plaintiffs' electronic communications. SmartDownload reported back to Defendants information about certain files that a given SmartDownload user downloaded from the Internet.

In the "Background" section of their brief, but not in their legal argument, Defendants wrongly assert that "Plaintiffs do not and cannot allege that [the unique

identification information transmitted by SmartDownload] could be used by Netscape to identify an actual person." Memorandum of Law in Support of Motions to Dismiss ("Def. Mem.") at 4 (emphasis added). As that is not an element of the ECPA, Plaintiffs need neither allege nor prove that fact[1] but, if they had to, they could allege and show at trial that Defendants could indeed associate the intercepted information with actual people. See, e.g., Treasury Board of Canada's "Cookie Guidelines," available at http://www.cio-dpi.gc.ca/pgol-pged/cookies-temoins/cookies-temoins02_e.asp (at Section B3 - "Privacy Concerns With Cookies").

Defendants also argue that the information that they surreptitiously obtained using SmartDownload was not "content" within the meaning of the ECPA. Plaintiffs address Defendants' inapposite legal authority in the Argument section below. The information that SmartDownload transmitted to Defendants could communicate the fact that the SmartDownload user was requesting specific content about specific subjects including[2]:

- birth control, abortion, or adoption (e.g., http://axtronic.gmxhome.de/birth-control/ef_natural-family-planning.htm, http://www.refuseandresist.org/ab/march10/2000/012900organiz.html, http://www.ferre.org/newbrow/adption4.html);
- recovery from chemical dependency or substance abuse such as 12-step programs (e.g., http://www.recovery-man.com/AA/index.htm, http://anonpress.org/pocketaa/, http://www.fare-wi.org/mfscwrkshp1.htm, http://hitspot.utk.edu/hit/main/reports/treatmentlist/2001/cover.htm);

---

1 Defendants do not (and cannot) assert that the failure to make that allegation renders Plaintiffs' claim legally deficient.

2 The URLs cited are for web pages containing links to relevant zip or exe files. If someone with SmartDownload installed on their computer downloaded one of these exe or zip files, SmartDownload would send the name and location of the file back to Defendants along with information uniquely identifying that user.

- protecting and saving children from child abuse (e.g., http://www.crv.gov.ab.ca/CRV.nsf/(Search)/Child+Abuse+and+Neglect-Private+Guardianship+Services);
- mental health (e.g., http://www.btinternet.com/~perrandoc/depress2.htm);
- financial or legal difficulties or issues (e.g., http://www.lawyerassistant.com/freeforms/index.html);
- physical health difficulties or issues (e.g., http://www.engenderhealth.org/res/onc/hiv/download.html);
- marital difficulties or issues (e.g., http://www.focusfamily.org.uk/lmm.html);
- sexual harassment (e.g., http://www.sexualharassmentpolicy.com/htm/federal_law.htm);
- sexual preferences or gender issues (e.g. http://www.qrd.org/qrd/www/orgs/axios/);
- minority religious views (e.g., http://www.itstime.com/swisdom3.htm);
- a competitor's web browser (e.g., http://www.microsoft.com/windows/ie/downloads/critical/ie6sp1/download.asp);
- online gambling software (e.g., http://www.online-gamblingsystems.com/order.htm); and
- many other things of potential interest to marketers, pollsters, hucksters, politicians, and law enforcement and other governmental agencies.

Defendants argue that Plaintiffs' action is supported by "a heavy dose of alarmist rhetoric." Def. Mem. at 1. Plaintiffs' principal point in this Memorandum is that Defendants' conduct, as fully alleged in the Complaints, violated both the letter and the spirit of the ECPA and the CFAA, as well as the underlying Constitutional principles that they embody. However, Plaintiffs respond briefly here to Defendants' rhetorical argument by noting that many people share Plaintiffs' alarm at the type of covert surveillance in which Defendants engaged and the erosion of personal freedom and civil liberties that acceptance of Defendants' arguments would entail. See, e.g., remarks in the 107th Congress in

connection with the re-introduction of the proposed Spyware Control and Privacy Protection Act:

> Quicken is not the only software program that may contain spyware. One computer expert recently found spyware programs in popular childrens' software that is designed to help them learn, such as Mattel Interactive's Reader Rabbit and Arthur's Thinking Games. And, according to another expert's assessment, spyware is present in four hundred software programs, including commonly used software such as RealNetworks RealDownload, Netscape/AOL Smart Download, and NetZip Download Demon. Spyware in these software programs can transmit information about every file you download from the Internet.

Statement of Sen. Edwards introducing S. 197, 147 Cong. Rec. S636-04 at S644-646, 2001 WL 69660 (Cong. Rec.) (107th Cong. Jan. 29, 2001); see also 146 Cong.Rec. E1949-04, 2000 WL 1598743 (Cong. Rec.) at E1949-1951 (106th Cong. Oct. 26, 2000) (Extension of Remarks by Rep. Holt). The use of spyware is reportedly growing. See John Borland, "A Secret War - Spike in Spyware Accelerates Arms Race," CNET News.com, February 24, 2003, available at http://news.com.com/2009-1023-985524.html.

In the Introduction Section of their Memorandum, Defendants also assert that the current version of SmartDownload does not send any file download information to Netscape. Def. Mem. at 1. They fail to note that they did not remove the surveillance mechanism from SmartDownload until after Plaintiffs had publicly disclosed the existence of that mechanism for the first time.

ARGUMENT

In their Memorandum, Defendants assert only four legal arguments. They argue that the information that they harvested using SmartDownload did not constitute the "contents" of a protected communication within the meaning of the ECPA. Def. Mem. at 8-

14. In fact, however, the information that SmartDownload intercepted and sent back to Netscape was rich in "content" within the meaning of the ECPA.

Defendants also assert that the Complaint does not allege that Plaintiff Specht was a party to a protected communication under the ECPA. Def. Mem. at 14-15. Defendants have simply missed the operative allegations, as detailed below.

Defendants assert that Plaintiff Specht has no standing to assert a claim under the ECPA for the interception of communications as to which he was the sole recipient, on the grounds that he was not the speaker of those communications. Def. Mem. at 15-17. They ignore the only authority on the subject, which is to the contrary.

Finally, Defendants assert that Plaintiffs fail to allege the $5,000 jurisdictional amount of "damage or loss" under the CFAA. Def. Mem. at 17-20. However, except for a single decision, which has been roundly criticized, all of the recent applicable authority permits the aggregation of the claims of all class members, and these greatly exceed the jurisdictional minimum.

Defendants concede, as they must, that their motion is addressed only to the face of the Complaints. Def. Mem. at 3 n.2 (citing Patel v. Searles, 305 F.3d 130, 134-135 (2d Cir. 2002). Under Fed. R. Civ. P. 8, the substantive allegations of a complaint should only contain "a short and plain statement of the claim showing that the pleader is entitled to relief."

A complaint is construed in the light most favorable to the plaintiff for purposes of a motion to dismiss. Hishon v. King & Spaulding, 467 U.S. 69, 73 (1984). All facts alleged by the plaintiff are to be taken as true. Id. A complaint should not be dismissed for failure to

state a claim unless "it appears beyond doubt that the plaintiff can prove no set of facts which would entitle him to relief." Conley v. Gibson, 355 U.S. 41, 45-46 (1957).

Defendants assert that their conduct "bear[s] no resemblance" to the conduct that the law was designed to illegalize. Def. Mem. at 2. They assert that the statutes at issue were written during an era when the type of communication at issue was unknown or obscure. See Def. Mem. at 2. In support of their position, Defendants cite the Senate Report on the ECPA, S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555. Def. Mem. at 9-10.[3]

That Report makes clear, however, that Defendants' conduct is precisely of the kind that the ECPA was enacted to prevent. It shows that the ECPA was drafted broadly, after the advent of email and computer networks, to which they are fully applicable by their unambiguous terms. They were expressly designed to illegalize or clarify the illegality of the very type of behavior in which Defendants engaged. See, e.g., 1986 U.S.C.C.A.N. 3557-3558 (the ECPA expands protections for "electronic mail and computer-to-computer communications"); id. at 3559-3560 (the statutory gap that the ECPA was designed to fill "may unnecessarily discourage potential customers from using innovative communications systems. It probably encourages unauthorized users to obtain access to communications to which they are not a party."). In addition to electronic mail and computer-to-computer communications, the ECPA was specifically designed to afford privacy protections to "electronic bulletin boards" and "remote computer services." See id. at 3562-3565.

---

[3] The CFAA was most recently amended in March of 2000 and Defendants do not argue that it does not address the types of violations alleged.

I.

SmartDownload Transmitted the "Contents" of Electronic Communications.

Defendants assert that the Complaint does not adequately allege that SmartDownload transmitted the "contents" of an electronic communication. Def. Mem. at 8-14.

The ECPA defines the "contents" of an electronic communication to include "any information concerning the substance, purport, or meaning of that communication." The Complaints allege that "[t]he file name, its source, and the Internet identities of the participants in that electronic communication constitute a part of the 'content' of that electronic communication . . . " See, e.g., Specht Complaint ¶ 47.

Defendants purport to quote the statutory definition, but they omit the word "any" from the beginning of the definition and prepend the word "only" before it, thereby turning a purely inclusive definition into a purely exclusive one. Def. Mem. at 8.

However, the information transmitted by SmartDownload still fits comfortably within Defendants' inverted definition. As noted in the Introduction above, the files that a SmartDownload user decides to download can provide rich, intimate details about that person's life. A user decides to download a particular zip or exe file because of the information that it contains. That is to say, he makes the decision based on the contents of the file. His request for the file, which was what SmartDownload was covertly transmitting back to Defendants when this action was instituted, therefore reflects the contents of the file that he is requesting. It is the exact electronic equivalent of saying, for example, "give

me your information package about 12-step programs." It is, in short, "the substance, purport, or meaning of that communication."

Defendants argue that the URL of the file that is transmitted by SmartDownload is more like a telephone number and less like the information communicated during the telephone call itself, and that recording a telephone number is not recording the "content" of the call. Def. Mem. at 10-13.

This argument does not withstand scrutiny. One problem with this argument is that, unlike the URLs of zip and exe files, recording telephone numbers is specifically excluded from the reach of the ECPA. 18 U.S.C. § 2511(2)(h).

Moreover, two people having a telephone conversation could be talking about anything at all, and so recording or transmitting the mere fact that Person "A" has called Person "B" provides no information at all about what they talked about. Unlike a telephone number, the URL of a zip file or exe file may literally speak volumes. Anybody who, like Defendants, intercepted the URL of the file that the SmartDownload user was downloading could then find out exactly what the requester requested and received by simply "dialing" the URL, retrieving the file, and reading it for himself. In essence, once Defendants learned the URL of a file downloaded by a SmartDownload user, they could see exactly what it was that he had requested, with absolute digital precision and clarity. In short, the URL is shorthand for a large amount of specific, detailed, and often quite sensitive information. In contrast, the fact that "A" and "B" spoke says nothing at all about the "contents" of that call. There is simply no valid analogy.

Defendants conclusorily assert that, since recording a telephone number by itself generally does not constitute an interception of the contents of the call, and since it is possible to call a "900" number that plays a recorded voice message, and since it is possible for someone who recorded the 900 number that was called to then call the number himself and hear the same recording, therefore the URLs of zip and exe files on the Internet lack content. Def. Mem. at 13.

As noted above, recording telephone numbers is an express statutory exception to the ECPA. However, there is another problem with this argument. Most telephone numbers do not have a recording, whereas most zip and exe files on the Internet contain substantive information and "say" exactly the same thing from "call" to "call." The statutory rule is that telephone numbers do not constitute content. However, if most telephone numbers had recorded messages, the rule would have to be that telephone numbers do constitute the contents of the communication, because if you knew the number that was called you would know exactly what was said, and if that is not content then nothing is.

Defendants assert that mere "transactional records" are not "contents." Def. Mem. at 9-12. However, they cite no case that holds that the URL of a zip or exe file is a mere transactional record. Nor can they, as the URL of such a file is much more informative than a record of what telephone number somebody called. [4]

---

[4] United States v. Allen, 53 M.J. 402 at 409 (C.A.A.F. 2000), the only authority cited by Defendants for the proposition that a URL is not "content," does not address the question. It merely holds that a governmental violation of the Stored Communications portion of the ECPA does not contain an exclusionary rule and so that portion did not preclude the introduction of evidence obtained in violation of that statute. Id.

Defendants also assert that the Complaints do not sufficiently plead that Defendants used the information that they harvested from the unsuspecting SmartDownload users. Def. Mem. at 8 n. 5. Under the ECPA, using an intercepted electronic communication is a separate violation from the interception itself. 18 U.S.C. §§ 2511(1), 2520(a); see Specht Complaint ¶¶ 42-44, 50. Defendants assert that Plaintiffs' allegations that Defendants not only "intercepted" the communications but that they also used them are "baldly conclusory." Def. Mem. at 8 n. 5. However, the Complaints assert that "SmartDownload's transmission of this data is functionally unrelated to its ability to resume downloads" and that Defendants concealed the transmission function from SmartDownload users. See, e.g., Specht Complaint ¶¶ 2, 40. SmartDownload was not designed to secretly send this data by accident. Defendants intended to put that information to use somehow. Plaintiffs need not allege what use Defendants intended because the nature of the use is not relevant to the existence of the violation. 18 U.S.C. §§ 2511(1), 2520(a). Defendants thus ask the Court to rule that allegations that they intentionally designed software to secretly collect information from their software users provide no basis for the assertion that they used any of that information. Plaintiffs submit that their allegations are sufficient.

II.

Mr. Specht was a Party to Intercepted Communications.

Defendants argue that the Specht Complaint fails to plead that Mr. Specht was a party to any intercepted communication. Def. Mem. at 14. They are simply mistaken. Specht Complaint ¶¶ 1, 2, 12, 14, 49.

Defendants also assert that the Specht Complaint does not allege that SmartDownload users who accessed Mr. Specht's site did not consent to the interception. Def. Mem. at 14-15. Of course, it is ancient, black letter law that a complaint need not anticipate and rebut affirmative defenses. Water-Works Co. v. Barret, 103 U.S. 516 (1881). But in any event, Defendants are again simply mistaken, as each Complaint expressly pleads lack of consent. E.g., Specht Complaint at ¶ 2:

> Unbeknownst to the members of the Class, and without their authorization, defendants have been spying on their Internet activities. "SmartDownload," a product distributed by defendants to users of Netscape's "Communicator" Web browser, is an electronic bugging device. It secretly intercepts electronic communications between Web users and Web sites - communications to which defendants are not a party. . . . SmartDownload captures and transmits this information without the consent of either the Web site or the Web user visiting the Web site. . . .

(emphasis added). See also Specht Complaint at ¶ 48 (SmartDownload operates "secretly").¶

III.

Mr. Specht Has Standing.

Defendants argue that Mr. Specht does not sufficiently allege that he was "[a] person whose . . . electronic communication [was] intercepted . . . " within the meaning of 18 U.S.C. § 2520(a). Def. Mem. at 15-17.

Mr. Specht's Complaint clearly asserts that Defendants intercepted his electronic communications. Specht Complaint ¶¶ 1, 2, 12, 14, 49. It therefore alleges that he is "[a] person whose . . . electronic communication [was] intercepted . . . " 18 U.S.C. § 2520(a).

Defendants' rejoinder is that Mr. Specht does not allege enough - that he must allege the technical details of why he asserts that he is "[a] person whose . . . electronic communication [was] intercepted . . . " See Def. Mem. at 15-17.

Mr. Specht has four responses. First, his Complaint need not plead such detail. See Fed. R. Civ. P. 8; Conley v. Gibson, supra. Whether he is in fact "[a] person whose . . . electronic communication [was] intercepted . . . " is a factual issue that exceeds his pleading burden. Id. Second, even if such detail were required, the statute confers standing merely by virtue of the fact, alleged in great detail in his Complaint, that Defendants caused SmartDownload to intercept and transmit to them copies of requests that users had directed to Mr. Specht's servers. Third, Mr. Specht would show at trial that any communication asking his server for a file was always preceded by a communication from the requesting computer to his server asking his server to confirm that it was online and ready to respond to file requests, and by a response from his server indicating its availability and readiness, among other things. Only after his server had communicated its availability and readiness and the requesting computer had received that communication from his server would the requesting computer then send the request for the file. See, e.g., British Telecom., PLC v. Prodigy Comm. Corp., 217 F. Supp. 2d 399 at 407 (S.D.N.Y. 2002). Therefore, the transmission of the file request necessarily indicated that Mr. Specht's server had communicated its availability and readiness to serve the file. Finally, Mr. Specht would show at trial that, because web servers such as his respond

automatically to such requests, the fact, covertly communicated to Defendants, that the user's computer had made the request also effectively transmitted the fact that Mr. Specht's server then supplied the file.

The second point requires elaboration. Defendants' construction that the statutory phrase "any person whose . . . electronic communication [was] intercepted . . . " confers standing only on the sender of a particular communication and not on the recipient of that communication ignores the plain meaning of the statute, the rest of the statute, its legislative history, case law, and common sense.

By its express terms, the statute protects the privacy of electronic communications. It takes two to communicate. One hand clapping is not communication, nor is a tree falling in a forest. The answer to the question "whose communication was intercepted?" is that it was the communication between the file requester and the file provider that was intercepted. Under the plain meaning of the statute, each has standing. Accordingly, the recipient of an electronic communication has standing under the ECPA to seek redress for an interception thereof. Fischer v. Mt. Olive Lutheran Church, Inc., 207 F. Supp. 2d 914 at 925-926 (W.D. Wis. 2002); see also Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623 at 634, 634 n.17 (E.D. Pa. 2001).

Indeed, the ECPA defines "electronic communication" to mean "any transfer of . . . intelligence of any nature transmitted in whole or in part by a[n] . . . electromagnetic . . . system . . ." 18 U.S.C. § 2510(12) (emphasis added). There can be no transfer without a transferee as well as a transferor. There can be no transmission without a receiver as well as a transmitter.

This conclusion is bolstered by the fact that the statute provides that, if either party to the electronic communication consents to the interception, then the interception will not be unlawful. 18 U.S.C. § 2511(2)(d). The statute thus protects the joint privacy of the parties to the electronic communication. If either party consents, there is nothing to protect. If neither party consents, the communication is protected.

The legislative history unambiguously supports this conclusion. S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, sets forth, with respect to the Stored Communications section of the ECPA, the following:

> For example, a computer mail facility authorizes a subscriber to access information in their portion of the facilities storage. Accessing the storage of other subscribers without specific authorization to do so would be a violation of this provision. Similarly, a member of the general public authorized to access the public portion of a computer facility would violate this action by intentionally exceeding that authorization and accessing the private portions of the facility.

1986 U.S.C.C.A.N. at 3590.

Acceptance of Defendants' argument would lead to absurd results - results totally at odds with the language and apparent purpose of the statute. Imagine a very slight twist to the case at bar. Suppose that, whenever a web surfer viewed a web page using Netscape's Navigator[5] browser, Navigator covertly reported back to Netscape exactly what files the remote server had sent to the surfer but not what the surfer had requested. Under Defendants' construction of the statute, the surfer would have no standing, even though

---

5 Netscape has now apparently changed the name of its browser back to its original name, i.e., "Netscape." For clarity and continuity, and to help distinguish the browser from the other components of the bundled software package formerly known as "Communicator," Plaintiffs will continue to use the term "Navigator" to refer to the browser, "Messenger" to refer to the email program, and "Communicator" to refer to the bundled package.

Defendants could tell exactly what request the surfer had made and exactly what he had gotten in response - information from which they could reconstruct the surfer's every move. Could there be any doubt that the surfer would be "[a] person whose . . . electronic communication [was] intercepted . . . "?

Emails often quote the email to which they are responding. Suppose that Defendants' Messenger email program secretly sent to Netscape a copy of each email that the Messenger user received. Is it not clear that the purpose of the ECPA is to give standing not only to the senders of those emails but also to the intended recipient - the Messenger user? Similarly, suppose that Messenger secretly sent to Netscape a copy of each email that the Messenger user sent. Is it not clear that the purpose of the ECPA is to give standing not only to the Messenger user who sent the emails but also to the recipients? According to S. Rep. No. 99-541, 1986 U.S.C.C.A.N. at 3590, and the Fischer and Fraser cases cited above, the answer is that both parties have standing. Fischer, 207 F. Supp. 2d at 925-926; Fraser, 135 F. Supp. 2d at 634, 634 n.17.

Defendants' argument that the portion of the ECPA that embodies an exclusionary rule for wrongful interception, Section 2511, protects a broader class of interceptees than the civil portion, Section 2520, is true but beside the point. The term "aggrieved person" in Section 2510(11) includes not only the parties to the interception but also "a person against whom the interception was directed." It contemplates a warrant under Section 2518, the criminal procedure section, which is the only section that uses the term "aggrieved person." It thus extends the criminal exclusionary rule to cover not only the parties to the communication wrongfully intercepted but also the subject of the warrant

wrongfully issued. The civil liability provision, Section 2520, simply does not assume anything about a warrant.

IV.

CFAA Claims May be Aggregated.

Plaintiffs plead economic damage under the CFAA as follows:

> Section 1030 defines the term "damage" to include "any impairment to the integrity or availability of . . . a system . . . that– . . . causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals . . ." 18 U.S.C. § 1030(e)(8)(A). By using SmartDownload to secretly obtain information contained in the computers of Class members about what files are downloaded, each defendant has caused "damage" within the meaning of § 1030.

E.g. Specht Complaint ¶ 60.

18 U.S.C. § 1030(a)(5)(A) provides in pertinent part:

> (a) Whoever –
>
> > (5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct intentionally causes damage without authorization, to a protected computer . . . shall be punished as provided in subsection (c) of this section

Defendants do not contest that the Complaints allege that they intentionally accessed Plaintiffs' computers without authorization as provided in the statute. Their sole argument with respect to Plaintiffs' CFAA claims is that Plaintiffs have not adequately alleged damage totaling $5,000 as is required under §1030(e)(8). In so arguing, Defendants incorrectly conclude that each Plaintiff is required to allege economic damages to his particular computer totaling at least $5,000 which results from a single act of unauthorized access.

Defendants' interpretation of the CFAA ignores the plain language of §1030(e)(8)(A), which allows for aggregation of damages by one or more individuals

over a one year time frame. In re AOL, Inc. Version 5.0 Software Litig., 168 F. Supp. 2d 1359 (S.D. Fla. 2001); Ingenix, Inc. v. Claude LaGalante, No. 02-876, 2002 U.S. Dist. Lexis 5795 (E.D. La. Mar. 28, 2002); In Re Toys R Us, Inc. Privacy Litig., MDL Nos. M-00-1381 MMC, C-00-2746 MMC, 2001 U.S. Dist. Lexis 16947 (N.D. Ca. Oct. 9, 2001).

Defendants rely chiefly on In Re Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001), a decision which has been criticized in a number of subsequent decisions as having misinterpreted the CFAA.

For example, the AOL decision found Doubleclick to be lacking in any "significant analysis" and wrong on the aggregation of damages issue. AOL, 168 F. Supp. 2d at 1373. AOL rejected the notion embraced in Doubleclick that a plaintiff could only aggregate damages as it related to a single computer. Because most computers are worth less than $5,000 individually, Defendants' aggregation argument would permit large online companies to violate the CFAA so long as they caused any single individual less than $4,999.99 in damages.

> If this court were to interpret 18 U.S.C.§1030(e)(8)(A) as requiring each home user to sustain more than $5,000 damage, the home user never would be protected because $5,000 is far more than the average price of a home computer system.
>
> AOL's interpretation . . . would lead to the absurd result that a party who accesses one computer without authorization, and thereby causes $5,000 worth of damage to that one computer, would be guilty of violating the CFAA and, therefore, civilly liable. On the other hand, a party who accesses millions of computers and causes only $100 worth of damage to each computer would not be guilty of violating the CFAA.

Id. at 1374. That reasoning is persuasive because it gives force to the letter and the spirit of the statute, which is "to prevent computer fraud that causes loss or injury." In re Intuit Privacy Litig., 138 F. Supp. 2d 1272 at 1281 (C.D. Ca. 2001).

Further, Defendants interpret "single act" to exclude its uniform practice of surreptitiously intercepting and recording Plaintiffs' and Class members' online information. This contorted understanding of the CFAA was criticized in AOL. Under Defendants' reasoning, uniform conduct affecting different computers does not constitute a single act and thus damages cannot be aggregated. AOL, as well as other decisions, have refused to interpret the CFAA so as to render it unenforceable by applying a single act aggregation bar. See, e.g., United States v. Morris, 928 F.2d 504, 506 (2d Cir. 1991) (affirming CFAA conviction of defendant who caused damage to several computers where estimated cost of damage ranged from $200 to $53,000).

Aggregation of damages is appropriate in the present case because Defendants' conduct constituted a "single act" as confirmed by the AOL court's ruling. AOL implicitly found that AOL's conduct – providing browsing software to millions of Internet users – was a single act. Consistent with the AOL decision, as well as the decision in Toys R US, Defendants' conduct in providing SmartDownload to millions of Internet users and the resulting automated recording and transmission of SmartDownload users' download information along with unique identification information, constitutes a single "act", notwithstanding that the information was collected at different times. It is that single act - by which Defendants exceeded their authorized access to the computers of millions of Smartdownload users, which allows Plaintiffs and the Class members to aggregate their damages for purposes of satisfying the $5,000 threshold.

Clearly, Defendants have sought to track Plaintiffs' activity on the Internet to gain an economic advantage. Plaintiffs' Complaints specifically reference such economic advantage:

> Thus, through SmartDownload's spying, AOL can obtain information about a) which Web users are looking into opening Internet access accounts with AOL's competitors; b) which Web site operators are assisting those competitors; and c) which Web site operators threaten the greatest potential loss of business to AOL.

E.g., Specht Complaint ¶ 37.

> Defendants are using SmartDownload to eavesdrop. They are using SmartDownload to intercept and obtain information about communications to which they are not a party. Moreover, by including the contents of the Netscape cookie and the SmartDownload Key in the transmission, they are intentionally providing themselves with all of the information that they need to create moment-by-moment profiles of file transactions by both individual Web users and individual Web sites.

E.g., Specht Complaint ¶ 38.

This information clearly has value to Defendants and, to the extent that it is being misappropriated from Plaintiffs, Plaintiffs ought to be compensated. Under similar factual circumstances, the Toys R Us decision reasoned that there is a very real economic value in such misappropriated information:

> Here, plaintiffs have alleged that the Coremetrics' cookie is a "specially formatted text file". (see Compl. At P36) which, unbeknownst to plaintiffs, defendants caused to be implanted in plaintiffs' computers. (See id. At P39). Plaintiffs further allege that they incurred, as a result of the implantation of that text file, the same type of damages, including misappropriation of the "economic value" of plaintiffs' "personalty," (see id. At P 59) and that such damages, in the aggregate, exceeded $5,000 during any one-year period. (see id. At P 86.) Liberally construed, these allegations are sufficient to allege that defendants caused an identical file to be implanted in each of the plaintiffs' computers, resulting in damages of a uniform nature. Such allegations are suffienct to allege the existence of a single act resulting in damages exceeding $5,000 during any one-year period to one or more individuals. See 18 U.S.C. §1030(e)(8)(A).

Toys R Us, 2001 U.S. Dist. Lexis 16947, at * 36.

Even Doubleclick, in dismissing claims for the unjust taking of the plaintiffs' personal information through the surreptitious tracking of their activity on the Internet, recognized the possibility that there can be economic value placed on such losses. See Doubleclick, 154 F. Supp.3d at 525-26. Indeed, had the Doubleclick decision properly permitted aggregation of damages among all computers and not just "a particular computer," the result in Doubleclick might well have been favorable to the plaintiff.

Finally, it is submitted that, should the Court agree that Plaintiffs, under the statute, are permitted to aggregate their damages, but finds that Plaintiffs' Complaints do not sufficiently describe facts supporting the economic losses attributable to the wrongful taking of Plaintiffs' information, Plaintiffs respectfully request leave to amend their Complaints to further amplify their allegations concerning their economic losses. See AOL, 168 F. Supp 2d 1359 (permitting the plaintiffs to amend their complaint in order to amplify their allegations concerning economic damages); see also Intuit, 138 F. Supp. 2d 1272 (plaintiffs who failed to allege economic damages in the complaint – either individually or in the aggregate - were permitted to amend their complaint).

CONCLUSION

For the reasons stated herein, Defendants' motion should be denied in its entirety.

Dated: March 4, 2003

ABBEY GARDY, LLP

By: _____
Joshua N. Rubin (JR 4118)
212 East 39th Street
New York, New York 10016
212-889-3700

Counsel for Plaintiffs

LAW OFFICES OF JAMES V. BASHIAN
James V. Bashian (JB-6331)
Oren S. Giskan (OG-3667)
500 Fifth Avenue
Suite 2800
New York, New York 10010
212-921-4110

Counsel for Plaintiff Sherry Weindorf

LEESFIELD, LEIGHTON, RUBIO & MAHFOOD
George G. Mahfood, Esq.
2350 South Dixie Highway
Miami, FL 33133

Counsel for Plaintiff Mark Gruber

OF COUNSEL

Laurence D. Paskowitz, Esq.
767 Third Avenue--35th Floor
New York, NY 10017-2023
212-486-6798

F:\CASES\NETSCAPE\MOTIONS\MOTDIS\BRIEFOP2.DOC

CERTIFICATE OF SERVICE

I, DENISE SCOTT, hereby certify that on this 4th day of March, 2003, I caused the following copy of our Plaintiffs' Amended Memorandum of Law in Opposition to Defendants' Motion to Dismiss to be served fax and federal express mail upon

WILMER, CUTLER & PICKERING
Roger W. Yoerges, Esq.
2445 M Street, N.W.
Washington, D.C. 20037-1420
Tel: (202) 663-6000
Fax: (202) 663-6363

Denise Scott

ABBEY GARDY, LLP

212 EAST 39TH STREET
NEW YORK, NEW YORK 10016

(212) 889-3700

FACSIMILE NUMBER:
(212) 684-5191
www.abbeygardy.com

ARTHUR N. ABBEY
JILL S. ABRAMS
KARIN E. FISCH
MARK C. GARDY*
JAMES S. NOTIS*
PAUL O. PARADIS*
STEPHEN T. RODD
JOSHUA N. RUBIN
JUDITH L. SPANIER

STEPHANIE AMIN-GIWNER**
CURT P. BECK
MICHAEL H. COHEN*
NANCY KABOOLIAN
EVAN J. KAUFMAN
ILANA KOHN&
RICHARD S. MARGOLIES
GIANNA M. MCCARTHY*

* ADMITTED TO NY & NJ
** ADMITTED TO MARYLAND ONLY
& ADMITTED TO CALIFORNIA ONLY

March 4, 2003

BY HAND

Honorable Alvin K. Hellerstein
United States District Court
Southern District of New York
910 U.S. Courthouse
500 Pearl Street
New York, New York 10007

Re: Specht v. Netscape Comm. Corp., 01-7860(L), 01-7870(CON), 01-7872(CON)

Dear Judge Hellerstein:

Enclosed please find a courtesy of Plaintiffs' Amended Memorandum of Law in Opposition to Defendants' Motion to Dismiss. The amendment is being made on consent of the Defendants to correct certain non-substantive errors in the table of authorities and case citations in the body of the brief.

Respectfully submitted,

Joshua N. Rubin

JNR:ds
Enclosure

cc:

Roger W. Yoerges, Esq.