UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In re DOUBLECLICK INC. PRIVACY LITIGATION,	:	Master File No. 00 Civ. 0641 (NRB)
This Document Relates To:	:	**OPINION AND ORDER**
ALL ACTIONS.	:	

NAOMI REICE BUCHWALD
UNITED STATES DISTRICT JUDGE

Plaintiffs bring this class action on behalf of themselves and all others similarly situated[1] against defendant DoubleClick, Inc. ("defendant" or "DoubleClick") seeking injunctive and monetary relief for injuries they have suffered as a result of DoubleClick's purported illegal conduct. Specifically, plaintiffs bring three claims under federal laws: (1) 18 U.S.C. §2701, et seq.; (2) 18 U.S.C. §2510, et seq.; (3) 18 U.S.C. §1030, et seq.; and four claims under state laws: (1) common law invasion of privacy; (2) common law unjust enrichment; (3) common law trespass to property; and (4) Sections 349(a) and 350 of Article 22A of the New York General Business Law.

Now pending is DoubleClick's motion, pursuant to Fed. R.

[1] The class is defined as "All persons who, since 1/1/96, have had information about them gathered by DoubleClick as a result of viewing any DoubleClick products or services on the Internet or who have had DoubleClick 'cookies,' as defined below, placed upon their computers." Plaintiffs' May 26, 2000 Amended Complaint ("Amended Complaint") at ¶1.

Civ. P. 12(b)(6), to dismiss Claims I, II and III of the Amended Complaint for failure to state a claim on which relief can be granted. For the reasons discussed below, DoubleClick's motion is granted and the Amended Complaint is dismissed with prejudice.

PROCEDURAL HISTORY

This case is a multidistrict consolidated class action. The initial complaint was filed in this Court on January 31, 2000. On May 10, 2000, this Court consolidated the set of related federal class actions against DoubleClick in the Southern and Eastern Districts of New York pursuant to Rule 42(a) of the Fed. R. Civ. P. and Local Rule 1.6 of the Southern and Eastern Districts of New York.[2] The consolidated class filed its Amended Complaint on May 26, 2000. Later, pursuant to 28 U.S.C. § 1407(a), the Judicial Panel on Multidistrict Litigation transferred two cases to this Court for pretrial proceedings:

---

[2] Healy v. DoubleClick, 00 Civ. 0641 (NRB); Donaldson v. DoubleClick, 00 Civ. 0696 (RMB); Wong v. DoubleClick, 00 Civ. 1253 (NRB); Mandel v. DoubleClick, 00 Civ. 1290 (RMB); Cohen v. DoubleClick, 00 Civ. 1349 (JSM); Katz v. DoubleClick, 00 Civ. 1552 (UN-RMB); Bruce v. DoubleClick, 00 Civ. 1572 (JGK); Gibson v. DoubleClick, 00 Civ. v1596 (U-RMB); Lehner v. DoubleClick, 00 Civ. 1813 (U-NRB); Gassman v. DoubleClick, 00 Civ. 1897 (U-NRB); Rand v. Doubleclick 00 Civ. 6398 (NRB).

Steinbeck v. DoubleClick, 00 Civ. 5705, C.A, N.O. 8:00-98 (C.D. Cal) on July 31, 2000 and Freedman v. DoubleClick, 00 Civ. 7194, 2:00-1559 (E.D. La) on September 22, 2000.

BACKGROUND[3]

DoubleClick, a Delaware corporation, is the largest provider of Internet advertising products and services in the world. Its Internet-based advertising network of over 11,000 Web publishers has enabled DoubleClick to become the market leader in delivering online advertising. DoubleClick specializes in collecting, compiling and analyzing information about Internet users through proprietary technologies and techniques, and using it to target online advertising. DoubleClick has placed billions of advertisements on its clients' behalf and its services reach the majority of Internet users in the United States.

THE INTERNET

Although a comprehensive description of the Internet is

[3] Unless otherwise noted, all facts are drawn from the Amended Complaint or are matters of which we take judicial notice.

unnecessary to address the issues raised in this motion, a rudimentary grasp of its architecture and engineering is important.[4] The Internet is accurately described as a "network of networks." Computer networks are interconnected individual computers that share information. Anytime two or more computer networks connect, they form an "internet." The "Internet" is a shorthand name for the vast collection of interconnected computer networks that evolved from the Advanced Research Projects Agency Network ("ARPANet") developed by the United States Defense Department in the 1960's and 1970's. Today, the Internet spans the globe and connects hundreds of thousands of independent networks.

The World Wide Web ("the Web" or "WWW") is often mistakenly referred to as the Internet. However, the two are quite different. The Internet is the physical infrastructure of the online world: the servers, computers, fiber-optic cables and routers through which data is shared online. The Web is data: a vast collection of documents containing text, visual images, audio clips and other information media that is accessed through the Internet. Computers known as "servers" store these documents and make them available over the Internet through

---

[4] See generally Reno v. ACLU, 521 U.S. 844 (1997) (description of the Internet).

“TCP/IP” (Transmission Control Protocol/Internet Protocol), a set of standard operating and transmission protocols that structure the Web’s operation. Every document has a unique “URL” (Universal Resource Locator) that identifies its physical location in the Internet’s infrastructure. Users access documents by sending request messages to the servers that store the documents. When a server receives a user’s request (for example, for Lycos.com’s home page), it prepares the document and then transmits the information back to the user.

The Internet utilizes a technology called “packet switching” to carry data. Packet switching works as follows. The computer wishing to send a document (“originating computer”), such as a music file or digital image, cuts the document up into many small “packets” of information. Each packet contains the Internet Protocol (“IP”) address of the destination Web site, a small portion of data from the original document, and an indication of the data’s place in the original document. The originating computer then sends all of the packets through its local network to an external “router.” A router is a device that contains continuously-updated directories of Internet addresses called “routing tables.” The router takes each packet from the original document and sends it to the next available router in the direction of the destination Web site. Because

each router is connected to many other routers and because the connection between any two given routers may be congested with traffic at a given moment, packets from the same document are often sent to different routers. Each of these routers, in turn, repeats this process, forwarding each packet it receives to the next available router in the direction of the destination Web site. Collectively, this process is called "dynamic routing."

The result is that packets of information from the originating computer may take entirely different routes over the Internet (i.e., traveling over different routers and cables) to their ultimate destination. Obviously, the packets arrive out of their original order because some have been forced to take much longer or slower routes between the originating and destination computers.[5] However, because each packet contains code that identifies its place in the original document, the destination computer is able to reassemble the original document from the disorganized packets. At that point, the destination computer sends a message back to the originating computer either

[5] For example, if a computer in New York sent a document to one in Boston, some packets might travel through routers and cables directly up the east coast while other packets might be sent by way of Seattle or Denver, due to momentary congestion on the east coast routes.

reporting that it received the full message, or requesting that the originating computer re-send any packets that never arrived. This entire process typically occurs in a matter of seconds. Packet-switching technology and dynamic routing have helped to give the Internet's infrastructure its extraordinary efficiency and resiliency.

DOUBLECLICK'S TECHNOLOGY AND SERVICES

DoubleClick provides the Internet's largest advertising service. Commercial Web sites often rent-out online advertising "space" to other Web sites. In the simplest type of arrangement, the host Web site (e.g., Lycos.com) rents space on its webpages to another Web site (e.g., TheGlobe.com) to place a "hotlink" banner advertisement[6] ("banner advertisment"). When a user on the host Web site "clicks" on the banner advertisement, he is automatically connected to the advertiser's designated Web site.

DoubleClick acts as an intermediary between host Web sites and Web sites seeking to place banner advertisements. It promises client Web sites that it will place their banner

---

[6] As plaintiffs explain, "Banner advertisements are so named because they generally resemble flags or banners, in that they tend to be long and narrow and their width often spans a significant part of a Web page." Amended Complaint at ¶60.

advertisements in front of viewers who match their demographic target. For example, DoubleClick might try to place banner advertisements for a Web site that sells golfclubs in front of high-income people who follow golf and have a track record of making expensive online purchases. DoubleClick creates value for its customers in large part by building detailed profiles of Internet users[7] and using them to target clients' advertisements.

DoubleClick compiles user profiles utilizing its proprietary technologies and analyses in cooperation with its affiliated Web sites. DoubleClick is affiliated with over 11,000 Web sites for which and on which it provides targeted banner advertisements. A select group of over 1,500 of these Web sites form the "DoubleClick Network" and are among "the most highly trafficked and branded sites on the Web." In addition, DoubleClick owns and operates two Web sites through which it also collects user data: (1) the Internet Address Finder ("IAF"); and (2) NetDeals.com.[8]

---

[7] It is important to note that the term "user" actually refers to a particular computer, not a particular person. DoubleClick collects information based upon the computer's Web activity, regardless of whether one person or one hundred people happen to use that computer. In the same vein, if one person uses multiple computers, DoubleClick would be unable to identify and aggregate the person's activity on different computers.

[8] Plaintiffs allege that IAF is marketed as the most comprehensive e-mail directory on the Internet. Netdeals.com is a "sweepstakes" and catalog Web site. Both Web sites allegedly

When users visit any of these DoubleClick-affiliated Web sites, a "cookie" is placed on their hard drives.[9] Cookies are computer programs commonly used by Web sites to store useful information such as usernames, passwords, and preferences, making it easier for users to access Web pages in an efficient manner. However, Plaintiffs allege that DoubleClick's cookies collect "information that Web users, including plaintiffs and the Class, consider to be personal and private, such as names, e-mail addresses, home and business addresses, telephone numbers, searches performed on the Internet, Web pages or sites visited on the Internet and other communications and information that users would not ordinarily expect advertisers to be able to collect." Amended Complaint at ¶38. DoubleClick's cookies store this personal information on users' hard drives until DoubleClick electronically accesses the cookies and uploads the data.

How DoubleClick targets banner advertisements and utilizes cookies to collect user information is crucial to our analysis under the three statutes. Therefore, we examine both processes in greater detail.

---

require users to submit personal information in order to use the services.

[9] If a DoubleClick cookie already exists on the user's hard drive, another is not placed.

A. Targeting Banner Advertisements

DoubleClick's advertising targeting process involves three participants and four steps. The three participants are: (1) the user; (2) the DoubleClick-affiliated Web site; (3) the DoubleClick server.[10] For the purposes of this discussion, we assume that a DoubleClick cookie already sits on the user's computer with the identification number "#0001."

In Step One, a user seeks to access a DoubleClick-affiliated Web site such as Lycos.com. The user's browser[11] sends a communication to Lycos.com (technically, to Lycos.com's server) saying, in essence, "Send me your homepage." U.S. Patent No. 5,948,061 (issued September 7, 1999) ("DoubleClick Patent"), col. 3, ll. 6-9. This communication may contain data submitted as part of the request, such as a query string or field information.

In Step Two, Lycos.com receives the request, processes it, and returns a communication to the user saying "Here is the Web page you requested." The communication has two parts. The first part is a copy of the Lycos.com homepage, essentially the collection article summaries, pictures and hotlinks a user sees

---

[10] DoubleClick actually has a great number of servers, but for the purpose of describing the process, it is easier to imagine just one.

[11] A browser is a computer program through which a user communicates on the Web.

on his screen when Lycos.com appears. The only objects missing are the banner advertisements; in their places lie blank spaces. Id. at col. 3, ll. 28-34. The second part of the communication is an IP-address link to the DoubleClick server. Id. at col. 3, ll. 35-38. This link instructs the user's computer to send a communication automatically to DoubleClick's server.

In Step Three, as per the IP-address instruction, the user's computer sends a communication to the DoubleClick server saying "I am cookie #0001, send me banner advertisements to fill the blank spaces in the Lycos.com Web page." This communication contains information including the cookie identification number, the name of the DoubleClick-affilated Web site the user requested, and the user's browser-type. Id. at col. 3, ll. 41-52.

Finally, in Step Four, the DoubleClick server identifies the user's profile by the cookie identification number and runs a complex set of algorithms based, in part, on the user's profile, to determine which advertisements it will present to the user. Id. at col. 3, ll. 52-57, col. 5, l. 11 - col. 6, l. 59. It then sends a communication to the user with banner advertisements saying "Here are the targeted banner advertisements for the Lycos.com homepage." Meanwhile, it also updates the user's profile with the information from the

request. Id. at col. 6, l. 60 - col. 7, l. 14.

DoubleClick's targeted advertising process is invisible to the user. His experience consists simply of requesting the Lycos.com homepage and, several moments later, receiving it complete with banner advertisements.

B. Cookie Information Collection

DoubleClick's cookies only collect information from one step of the above process: Step One. The cookies capture certain parts of the communications that users send to DoubleClick-affiliated Web sites. They collect this information in three ways: (1) "GET" submissions, (2) "POST" submissions, and (3) "GIF" submissions.

GET information is submitted as part of a Web site's address or "URL," in what is known as a "query string." For example, a request for a hypothetical online record store's selection of Bon Jovi albums might read: http://recordstore.hypothetical.com/search?terms=bonjovi. The URL query string begins with the "?" character meaning the cookie would record that the user requested information about Bon Jovi.

Users submit POST information when they fill-in multiple blank fields on a webpage. For example, if a user signed-up for

an online discussion group, he might have to fill-in fields with his name, address, email address, phone number and discussion group alias. The cookie would capture this submitted POST information.

Finally, DoubleClick places GIF tags on its affiliated Web sites. GIF tags are the size of a single pixel and are invisible to users. Unseen, they record the users' movements throughout the affiliated Web site, enabling DoubleClick to learn what information the user sought and viewed.

Although the information collected by DoubleClick's cookies is allegedly voluminous and detailed, it is important to note three clearly defined parameters. First, DoubleClick's cookies only collect information concerning users' activities on DoubleClick-affiliated Web sites.[12] Thus, if a user visits an

---

[12] See Amended Complaint at ¶6 ("Thus, through DoubleClick's relationships with Web publishers and advertisers located throughout the United States, defendant has secretly obtained personal and private information from plaintiffs and the Class members."); ¶42 ("When a user visits a Web site utilizing DoubleClick's advertising products and services..."); ¶45 ("DoubleClick's technology wrongfully monitors Internet users' activities at **each and every** Web site the users visit at which DoubleClick's products or services are utilized."); ¶68 ("Once DoubleClick implants a cookie onto a user's computer, DoubleClick is automatically able to access, read and update that cookie on any of the other 11,000 or so Web sites where it has a presence..."); Transcript of February 22, 20001 Oral Argument at 7-8 (admission by plaintiffs' counsel that information is only collected from DoubleClick-affiliated Web sites).

unaffiliated Web site, the DoubleClick cookie captures no information. Second, plaintiff does not allege that DoubleClick ever attempted to collect <u>any</u> information other than the GET, POST, and GIF information submitted by users. DoubleClick is never alleged to have accessed files, programs or other information on users' hard drives. Third, DoubleClick will not collect information from any user who takes simple steps to prevent DoubleClick's tracking. As plaintiffs' counsel demonstrated at oral argument, users can easily and at no cost prevent DoubleClick from collecting information from them. They may do this in two ways: (1) visiting the DoubleClick Web site and requesting an "opt-out" cookie; and (2) configuring their browsers to block any cookies from being deposited. Transcript of February 22, 2001 Oral Argument at 15-18.

Once DoubleClick collects information from the cookies on users' hard drives, it aggregates and compiles the information to build demographic profiles of users. Plaintiffs allege that DoubleClick has more than 100 million user profiles in its database. Exploiting its proprietary Dynamic Advertising Reporting & Targeting ("DART") technology, DoubleClick and its licensees[13] target banner advertisements using these demographic

---

[13] DoubleClick allegedly licenses its DART technology to thousands of Web sites who utilize it to target banner

profiles.

ABACUS ACQUISITION AND FTC INVESTIGATION

In June 1999, DoubleClick purchased Abacus Direct Corp. ("Abacus") for more than one billion dollars. Abacus was a direct-marketing services company that maintained a database of names, addresses, telephone numbers, retail purchasing habits and other personal information on approximately ninety percent of American households, which it sold to direct marketing companies. Plaintiffs allege that DoubleClick planned to combine its database of online profiles with Abacus' database of offline customer profiles in order to create a super-database capable of matching users' online activities with their names and addresses.

In furtherance of this effort, DoubleClick created the Abacus Online Alliance ("Abacus Alliance") and amended its privacy policy. The Abacus Alliance is purportedly a confidential group of online marketers and publishers who secretly contribute their compiled customer data to a cooperative database managed by DoubleClick. In return for their contributions, Abacus Alliance members gain access to exclusive DoubleClick products and services. In mid-1999,

---

advertisements on their own.

shortly after acquiring Abacus, DoubleClick amended its privacy policy by removing its assurance that information gathered from users online would not be associated with their personally identifiable information.

Not long after the Abacus acquisition, the Federal Trade Commission ("FTC") launched an investigation into whether DoubleClick's collection, compilation and use of consumer information constituted unfair or deceptive trade practices in violation of Section 5 of the Federal Trade Commission Act.[14] On March 2, 2000, Kevin O'Connor, DoubleClick's CEO and Chairman of the Board, announced that he had made a "mistake" by planning to merge DoubleClick's and Abacus' databases and stated that DoubleClick would undertake no such merger until it reached an agreement with the United States government and Internet industry regarding privacy standards. It is unclear whether

---

[14] Specifically, "[t]he primary purposes of the inquiry were: 1) whether [DoubleClick] used or disclosed consumers' PII [personal identifying information] for purposes other than those disclosed in, or in contravention of, its privacy policy, including in particular, whether it combined PII from Abacus Direct (an offline direct marketing company that it had acquired) with non-PII clickstream data that DoubleClick had collected; and 2) whether [DoubleClick] used or disclosed sensitive information about consumers in contravention of its stated privacy policy." Letter from Joel Winston, Acting Associate Director, Division of Financial Practices, FTC, to Christine Varney, Esq., Hogan & Hartson, Outside Counsel for DoubleClick, January 22, 2001 ("FTC January 22, 2001 Letter.").

DoubleClick had already merged any of the information.[15]

The FTC concluded its investigation on January 22, 2001. In a letter to DoubleClick's outside counsel, the FTC announced that it was ending its investigation with no finding that DoubleClick had engaged in unfair or deceptive trade practices. It summarized its conclusions:

> Based on this investigation, it appears to staff that DoubleClick never used or disclosed consumers' PII [personal identifiable information] for purposes other than those disclosed in its privacy policy. Specifically, it appears that DoubleClick did not combine PII from Abacus Direct with clickstream collected on client Web sites. In addition, it appears that DoubleClick has not used sensitive data for any online preference marketing product, in contravention of its stated online policy. We understand that DoubleClick's Boomerang product takes user data from one site to target advertising to the same user on other sites. However, the user profiles DoubleClick creates for its Boomerang clients for this targeting contains only non-PII. Furthermore, we understand that for all new Boomerang clients, DoubleClick requires by contract that the site disclose in its privacy policy that it uses DoubleClick's services to target advertising to consumers, and DoubleClick will not implement Boomerang on a site until such disclosures are

---

[15] Plaintiffs allege that in February 2000 (prior to O'Connor's announcement), DoubleClick President Kevin Ryan stated that DoubleClick had already merged between 50,000 and 100,000 records from online and offline databases. Amended Complaint at ¶82. However, the FTC, in its January 22,2001 letter ending its DoubleClick investigation, found "[s]pecifically, it appears that DoubleClick did not combine PII from Abacus Direct with clickstream collected on client Web sites." For the purposes of this motion, we assume the truth of plaintiffs' pleadings.

posted.[16]

The letter also noted several commitments DoubleClick made to modifying its privacy policy to "enhance its effectiveness," including allowing a user to request an "opt out" cookie that would prevent DoubleClick from collecting information from that user.

DISCUSSION

Defendants move to dismiss plaintiffs' claims, pursuant to Fed. R. Civ. P. 12(b)(6), for failure to state a claim upon which relief may be granted. In considering a motion to dismiss pursuant to Fed. R. Civ. P. 12(b)(6), we accept as true all material factual allegations in the Amended Complaint, Atlantic Mutual Ins. Co. v. Balfour Maclaine Int'l, Ltd., 968 F.2d 196, 198 (2d Cir. 1992), and may grant the motion only where "it appears beyond doubt that the plaintiff can prove no set of facts in support of his claim which would entitle him to relief." Still v. DeBuono, 101 f.3d 888, 891 (2d Cir. 1996); see Conley v. Gibson, 355 U.S. 41, 48 (1957). "General, conclusory allegations need not be credited, however, when they

[16] FTC January 22, 2001 Letter.

are belied by more specific allegations of the complaint." Hirsch v. Arthur Andersen & Co., 72 F.3d 1085 (2d Cir. 1995)(citing Jenkins v. S & A Chaissan & Sons, Inc., 449 F.Supp. 216, 227 (S.D.N.Y. 1978); 5A Charles A. Wright & Arthur R. Miller, Federal Practice and Procedure § 1363, at 464-65 (2d ed. 1990). In addition to the facts set forth in the Amended Complaint, we may also consider documents attached thereto and incorporated by reference therein, Automated Salvage Transp., Inc. v. Wheelabrator Envtl. Sys., Inc., 155 F.3d 59, 67 (2d. Cir. 1998), matters of public record such as case law and statutes, Pani v. Empire Blue Cross Blue Shield, 152 F.3d 67, 75 (2d. Cir. 1998), and matters of judicial notice. See Brass v. American Film Technologies, Inc., 987 F.2d 142, 150 (2d Cir. 1993); Kramer v. Time Warner Inc., 937 F.2d 767, 774 (2d Cir. 1991).

Claim I. Title II of the ECPA

Title II ("Title II") of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §2701 et. seq. ("§2701"), aims

to prevent hackers from obtaining, altering or destroying certain stored electronic communications. See Sherman & Co. v. Salton Maxim Housewares, Inc., 94 F.Supp.2d 817, 820 (E.D. Mich. 2000) ("the ECPA was primarily designed to provide a cause of action against computer hackers")(quoting State Wide Photocopy Corp. v. Tokai Fin. Serv., Inc., 909 F.Supp. 137, 145 (S.D.N.Y. 1995)). It creates both criminal sanctions and a civil right of action[17] against persons who gain unauthorized access to communications facilities and thereby access electronic communications stored incident to their transmission. Title II specifically defines the relevant prohibited conduct as follows:

> "(a) **Offense**. Except as provided in subsection (c) of this section whoever– (1) intentionally accesses without authorization a facility through which an electronic information service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains... access to a wire or electronic communication while it is in electronic storage in such system shall be punished...."

Plaintiffs contend that DoubleClick's placement of cookies on plaintiffs' hard drives constitutes unauthorized access and, as a result, DoubleClick's collection of information from the

---

[17] 18 U.S.C. §2707 ("§2707") creates a civil action against ECPA violators by "any provider of electronic communication service, subscriber, or other person aggrieved by a violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind..."

cookies violates Title II. However, Title II contains an exception to its general prohibition.

> "(c) **Exceptions.**-Subsection (a) of this section does not apply with respect to conduct authorized-...(2) by a user of that [wire or electronic communications] service with respect to a communication of or intended for that user;"

DoubleClick argues that its conduct falls under this exception. It contends that the DoubleClick-affiliated Web sites are "users" of the Internet and that all of plaintiffs' communications accessed by DoubleClick's cookies have been "of or intended for" these Web sites. Therefore, it asserts, the Web sites' authorization excepts DoubleClick's access from §2701(a)'s general prohibition.

We must first address the threshold issue of whether DoubleClick's argument that its conduct falls under a statutory exception is resolvable on a motion to dismiss. Plaintiffs contend that the issue turns on whether exception §2701(c)(2) is considered an affirmative defense or a statutory element of the offense. As a general matter, a plaintiff need not plead denials of affirmative defenses, see Harris v. City of New York, 186 F.3d 243, 251 (2d Cir. 1999)(citing 5 Charles Wright & Arthur Miller, Federal Practice and Procedure: Civil 2d § 1276 (2d ed. 1990 & 1999 pocket part)), whereas courts may dismiss a

claim based on a statutory exception that appears on the face of the complaint. See Orton v. Pirro, Collier, et al., No. 95 Civ. 3056, 1996 WL 18831, at *2 (S.D.N.Y. Jan. 18, 1996) (dismissing ECPA Title III claim where statutory consent exception appeared in the complaint).

Examining the statute, it appears that §2701(c) is a statutory exception. First, §2701(c) is entitled "Exceptions" and states "Subsection (a) of this section does not apply with respect to conduct..." Second, §2701(a) reinforces §2701(c)'s function by carving our §2701(c)'s exceptions in the very definition of the offense: "§2701(a) **Offense.**-Except as provided in subsection (c) of this section..." Third, §2707, the section that provides for a civil cause of action, subsection (e), is entitled "Defense" and specifies three affirmative defenses to civil claims under §2707. Presumably, if Congress had intended §2701(c)(1-3) to constitute affirmative defenses, it could have labeled them as such as it did in §2707. Fourth, nothing in the legislative history suggests that §2701(c) should be considered an affirmative defense instead of a statutory exception. Thus, if DoubleClick's conduct falls into one of §2701(c)'s exceptions on the face of the pleadings, it is proper for us to dismiss the claim as one within a statutory exception. Furthermore, even if §2701(c) was construed as an affirmative defense, the Second

Circuit has held that a court may properly dismiss a claim on the pleadings when an affirmative defense appears on its face. See Day v. Moscow, 955 F.2d 807, 811 (2d Cir. 1992)("[W]hen all relevant facts are shown by the court's own records, of which the court takes notice, the [affirmative] defense may be upheld on a Rule 12(b)(6) motion without requiring an answer"); see generally 2 James Wm. Moore et al., Moore's Federal Practice §12.34[4][b] (3d ed. 2000).

Assuming that the communications are considered to be in "electronic storage," it appears that plaintiffs have adequately pled that DoubleClick's conduct constitutes an offense under §2701(a), absent the exception under §2701(c)(2). Therefore, the issue is whether DoubleClick's conduct falls under §2701(c)(2)'s exception. This issue has three parts: (1) what is the relevant electronic communications service?; (2) were DoubleClick-affiliated Web sites "users" of this service?; and (3) did the DoubleClick-affiliated Web sites give DoubleClick sufficient authorization to access plaintiffs' stored communications "intended for" those Web sites?

A. "Internet Access" is the relevant electronic communications service.

Obviously, in a broad sense, the "Internet" is the relevant

communications service.[18] However, for the purposes of this motion, it is important that we define Internet service with somewhat greater care and precision. Plaintiff, at turns, argues that the electronic communications service is "Internet access" and "the ISP [Internet Service Provider]." Plaintiffs' Opposition Brief at 8, 12. The difference is important. An ISP is an entity that provides access to the Internet; examples include America Online, UUNET and Juno. Access to the Internet is the service an ISP provides. Therefore, the "service which provides to users thereof the ability to send or receive wire or electronic communications" is "Internet access."

B. Web Sites are "users" under the ECPA.

The ECPA defines a "user" as "any person or entity who (A) uses an electronic communication service; and (B) is duly authorized by the provider of such service to engage in such use." 18 U.S.C. §2510(13). On first reading, the DoubleClick-

[18] The ECPA defines "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. §2510(15). In turn, "electronic communications" are defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric, or photooptical system that affects interstate or foreign commerce." 18 U.S.C. §2510(12).

affiliated Web sites appear to be users -- they are (1) "entities" that (2) use Internet access and (3) are authorized to use Internet access by the ISPs to which they subscribe. However, plaintiffs make two arguments that Web sites nevertheless are not users. Both are unpersuasive.

First, plaintiffs argue that "[t]he most natural reading of 'user' is the person who has signed up for Internet access, which means the individual plaintiffs and Class members - not the Web servers." Plaintiffs' Opposition Brief at 12. Insofar as this argument implies that the statute meant to differentiate between human and non-human users, it is clearly contradicted by the statute's language that defines a "user" as "any person or entity..." (emphasis added). Furthermore, it rests on the erroneous assumption that only human users "sign[] up for Internet access," not Web sites or servers. This court takes judicial notice of the fact that all people and entities that utilize Internet access subscribe to ISPs or are ISPs. Although the vast majority of people who sign-up for Internet access from consumer-focused ISPs such as America Online and Juno are individuals, every Web site, company, university, and government agency that utilizes Internet access also subscribes to an ISP or is one. These larger entities generally purchase "Internet access" in bulk from ISPs, often with value-added services and

technologically advanced hardware. Nevertheless, they purchase the same underlying Internet access as individual users. Therefore, plaintiffs fail to distinguish class members from Web sites and servers based on whether they subscribe to an ISP for Internet access.

Second, plaintiffs argue that "[t]he individual plaintiff ('user') owns the personal computer ('facility'), while the Web sites she visits do not. [And that] [u]nder basic property and privacy notions, therefore, only she can authorize access to her own messages stored on that facility." Plaintiffs' Opposition Brief at 12. Again, plaintiffs seem to ignore the statute's plain language. The general rule under §2701(a) embodies plaintiffs' position that only those authorized to use a "facility" may consent to its access. Nevertheless, Congress explicitly chose to make §2701(a)'s general rule subject to §2701(c)(2)'s exception for access authorized by authors and intended recipients of electronic communications. Thus, plaintiffs' argument is essentially that this Court should ignore §2701(c)(2) because Congress failed to take adequate account of "basic property and privacy notions." However, it is not this Court's role to revisit Congress' legislative judgments.

One final point bears mention, even though plaintiffs did not raise it. One could imagine a facially sensible argument

that Web sites are not “users” of Internet access because they are passive storage receptacles for information; the human is the “user” and the Web site is what is used. However, the Internet’s engineering belies this description. Because the Internet functions through packet-switching and dynamic routing, human users do not in any sense connect to a passive receptacle and obtain information. Indeed, no direct connection ever exists between the human user and the Web site. Rather, the human user sends a request to which the Web site must actively respond: processing the request, deciding whether to provide the information sought, obtaining the document from the server, translating the document into TCP/IP protocol, sending the packets and awaiting confirmation of their arrival. Indeed, in a practical sense, Web sites are among the most active “users” of Internet access -- their existence and utility depend on it, unlike humans. Therefore, we find as a matter of law that the DoubleClick-affiliated Web sites are “users” of Internet access under the ECPA.

C. All of the communications DoubleClick has accessed through its cookies have been authorized or have fallen outside of Title II’s scope.

Because plaintiffs only allege that DoubleClick accessed communications from plaintiffs to DoubleClick-affiliated Web

sites, the issue becomes whether the Web sites gave DoubleClick adequate authorization under §2701(c)(2) to access those communications. This issue, in turn, has two parts: (1) have the DoubleClick-affiliated Web sites authorized DoubleClick to access plaintiffs' communications to them?; and (2) is that authorization sufficient under §2701(c)(2)?

1. The DoubleClick-affiliated Web sites have consented to DoubleClick's interception of plaintiffs' communications.

A plaintiff cannot survive a motion to dismiss a Title II claim based solely on the naked allegation that defendant's access was "unauthorized." A plaintiff must, "allege[] and proffer[] sufficient proofs to create a colorable claim that such access was 'unauthorized.'" See Sherman & Co. v. Salton Maxim Housewares, Inc., 94 F.Supp.2d 817,820-821 (E.D.Mich. 2000) (denying motion to amend complaint because "proposed claim under the ECPA does not state a claim," despite the fact plaintiff alleged access was unauthorized); cf. Hirsch v. Arthur Andersen & Co., 72 F.3d 1085 (2d Cir. 1995) ("General, conclusory allegations need not be credited, however, when they are belied by more specific allegations of the complaint.")(citation omitted). In the instant case, plaintiffs have proffered no proofs whatsoever to support their bare assertion that

Doubleclick's access was unauthorized. What is more, every fact they do allege supports the inference that the DoubleClick-affiliated Web sites did authorize DoubleClick's access.

Examining DoubleClick's technological and commercial relationships with its affiliated Web sites, we find it implausible to infer that the Web sites have not authorized DoubleClick's access. In a practical sense, the very reason clients hire DoubleClick is to target advertisements based on users' demographic profiles. DoubleClick has trumpeted this fact in its advertising, patents and Securities and Exchange filings. See infra notes 28-29 and accompanying text. True, officers of certain Web sites might not understand precisely how DoubleClick collects demographic information through cookies and records plaintiffs' travels across the Web. However, that knowledge is irrelevant to the authorization at issue -- Title II in no way outlaws collecting personally identifiable information or placing cookies, qua such. All that the Web sites must authorize is that DoubleClick access plaintiffs' communications to them. As described in the earlier section "Targeting Banner Advertisements," the DoubleClick-affiliated Web sites actively notify DoubleClick each time a plaintiff sends them an electronic communication (whether through a page request, search, or GIF tag). The data in these notifications (such as the name of the

Web site requested) often play an important role in determining which advertisements are presented to users. Plaintiffs have offered no explanation as to how, in anything other than a purely theoretical sense, the DoubleClick-affiliated Web sites could have played such a central role in the information collection and not have authorized DoubleClick's access. This purely theoretical possibility that a DoubleClick-affiliated Web site might have been so ignorant as to have been unaware of the defining characteristic of DoubleClick's advertising service -- the service the Web site knowingly and purposely purchased -- and its own role in facilitating that service, is too remote to be the basis for extensive and costly discovery of DoubleClick and its affiliates. Therefore, we find that the DoubleClick-affiliated Web sites consented to DoubleClick's access of plaintiffs' communications to them.

2. DoubleClick is authorized to access plaintiffs' GET, POST and GIF submissions to the DoubleClick-affiliated Web sites.

Plaintiffs' GET, POST and GIF submissions to DoubleClick-affiliated Web sites are all "intended for" those Web sites. In the case of the GET and POST submissions, users voluntarily type-in information they wish to submit to the Web sites, information

such as queries, commercial orders, and personal information. GIF information is generated and collected when users use their computer "mouse" or other instruments to navigate through Web pages and access information. Although the users' requests for data come through clicks, not keystrokes, they nonetheless are voluntary and purposeful. Therefore, because plaintiffs' GET, POST and GIF submissions to DoubleClick-affiliated Web sites are all "intended for" those Web sites, the Web sites' authorization is sufficient to except DoubleClick's access under §2701(c)(2).

3. To the extent that the DoubleClick cookies' identification numbers are electronic communications, (1) they fall outside of Title II's scope, and (2) DoubleClick's access to them is otherwise authorized.

Plaintiffs argue that even if DoubleClick's access to plaintiffs' GET, POST and GIF submissions is properly authorized under §2701(c)(2), the cookie identification numbers that accompany these submissions[19] are not because they are never sent to, or through, the Web sites. However, this argument too is unavailing.

(a) The Cookies' identification numbers are not in "electronic storage" and therefore are outside Title II's scope.

---

[19] This occurs in Step Three of the process as earlier described. See supra "Targeting Banner Advertisements."

Putting aside the issue of whether the cookie identification numbers are electronic communications at all, DoubleClick does not need anyone's authority to access them. The cookies' long-term residence on plaintiffs' hard drives places them outside of §2510(17)'s definition of "electronic storage" and, hence, Title II's protection. Section 2510(17) defines "electronic storage" as:

> "**(A)** any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
>
> **(B)** any storage of such communication by an electronic communication service for the purpose of backup protection of such communication." (emphasis added)

Clearly, the cookies' residence on plaintiffs' computers does not fall into §2510(17)(B) because plaintiffs are not "electronic communication service" providers.[20]

Section 2510(17)(A)'s language and legislative history make evident that "electronic storage" is not meant to include DoubleClick's cookies either. Rather, it appears that the

---

[20] 18 U.S.C. §2510(15) defines an "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." Examples of providers in the Internet world would include ISPs such as America Online, Juno and UUNET, as well as, perhaps, the telecommunications companies whose cables and phone lines carry the traffic. Nowhere do plaintiffs allege that they are electronic service providers or allege facts that could give rise to this inference.

section is specifically targeted at communications temporarily stored by electronic communications services incident to their transmission –- for example, when an email service stores a message until the addressee downloads it. The statute's language explicitly refers to "temporary, intermediate" storage. Webster's Dictionary defines "temporary" as "lasting for a limited time," and "intermediate" as "being or occurring at the middle place...." Webster's Third New International Dictionary 2353, 1180 (1993). In other words, Title II only protects electronic communications stored "for a limited time" in the "middle" of a transmission, i.e. when an electronic communication service temporarily stores a communication while waiting to deliver it.

The legislative history reveals that Congress intended precisely this limited definition. In H. Rpt. 106-932 (2000), a House Report on a proposed amendment to Title II, the House Judiciary Committee explained that "'(A)ny temporary, intermediate storage' [in §2510(17)(A)] describes an e-mail message that is being held by a third party Internet service provider until it is requested to be read." Id. at note 6 (emphasis added). This definition is consistent with Congress' statements in 1986, when it passed the ECPA. Sen. Rep. No. 99-541 (1986)'s entire discussion of Title II deals only with

facilities operated by electronic communications services such as "electronic bulletin boards" and "computer mail facilit[ies]," and the risk that communications temporarily stored in these facilities could be accessed by hackers. It makes no mention of individual users' computers, the issue in the instant case. Finally, Senator Patrick Leahy, a sponsor of the ECPA in 1986, recently proposed an amendment to the definition of "electronic storage" meant to clarify its scope. He proposed amending 2510(17)(A) to read:

> (17) ["**interim storage**"] means–
>
> > (A) any temporary, intermediate storage [**by an electronic communication service**] of a wire or electronic communication incidental to the electronic transmission thereof..." S. 106-3083, Sec. 3(a)(4) (2000).

This amendment lends further support to the conclusion that Congress' intent was to protect communications held in interim storage by electronic communication service providers.

Turning to the facts of this case, it is clear that DoubleClick's cookies fall outside §2510(17)'s definition of electronic storage and, hence, §2701's scope. Plaintiffs plead that in contrast to most cookies' ephemeral existence, DoubleClick cookies remain on plaintiffs' computers "for a virtually indefinite time period," and that their indefinite

existence is critical to their function.[21] Amended Complaint at ¶68. In plain language, "indefinite" existence is the opposite of "temporary," and the DoubleClick cookies's residence on plaintiffs' hard drives is certainly not an "intermediate" step in their transmission to another addressee. This plain language controls in the absence of any legislative history suggesting that Congress intended it to cover conduct like DoubleClick's. Indeed, if §2510(17) were interpreted in the manner plaintiffs advocate, Web sites would commit federal felonies every time they accessed cookies on users' hard drives, regardless of whether those cookies contained any sensitive information. This expansive reading of a criminal statute runs contrary to the canons of statutory interpretation and Congress' evident intent. See Jones v. United States, 120 S.Ct. 1904, 1907 (2000) ("Ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity [citation omitted], and when choice must be made between two readings of what conduct Congress has made a crime, it is appropriate, before choosing the harsher

---

[21] We note plaintiffs' allegation that the DoubleClick-affiliated Web sites' responses to plaintiffs' requests are "placed in temporary, immediate [sic] storage on the client [plaintiffs'] computers incidental to the transmission of such electronic communications." Amended Complaint at ¶56. However, this allegation clearly does not encompass the cookies or their identification numbers because neither are ever sent from the DoubleClick-affiliated Web sites to plaintiffs.

alternative, to require that Congress should have spoken in language that is clear and definite. [citation omitted]"); Lurie v. Wittner, 228 F.3d 113, 125-6 (2nd Cir. 2000). Thus, because the cookies and their identification numbers are never in "electronic storage" under the ECPA, they are not protected by Title II and DoubleClick cannot be held liable for obtaining them.

(b) If the DoubleClick cookies' identification numbers are considered stored electronic communications, they are "of or intended for" DoubleClick and DoubleClick's acquisition of them does not violate Title II.

Even if we were to assume that cookies and their identification numbers were "electronic communication[s]... in electronic storage," DoubleClick's access is still authorized. Section 2701(c)(2) excepts from Title II's prohibition access, authorized by a "user," to communications (1) "of" (2) "or intended for" that user. In every practical sense, the cookies' identification numbers are internal DoubleClick communications -- both "of" and "intended for" DoubleClick. DoubleClick creates the cookies, assigns them identification numbers, and places them on plaintiffs' hard drives. The cookies and their identification numbers are vital to DoubleClick and meaningless to anyone else. In contrast, virtually all plaintiffs are unaware that the cookies exist, that these cookies have identification numbers,

that DoubleClick accesses these identification numbers and that these numbers are critical to DoubleClick's operations.

In this sense, cookie identification numbers are much akin to computer bar-codes or identification numbers placed on "business reply cards" found in magazines. These bar-codes and identification numbers are meaningless to consumers, but are valuable to companies in compiling data on consumer responses (e.g. from which magazine did the consumer get the card?). Although consumers fill-out business reply cards and return them to companies by mail, the bar-codes and identification numbers that appear on the cards are purely internal administrative data for the companies. The cookie identification numbers are every bit as internal to DoubleClick as the bar-codes and identification numbers are to business reply mailers. Therefore, it seems both sensible to consider the identification numbers to be "of or intended for" DoubleClick and bizarre to describe them as "of or intended for" plaintiffs. Accordingly, because the identification numbers are "of or intended for" DoubleClick, it does not violate Title II for DoubleClick to obtain them from plaintiffs' electronic storage.

To summarize, plaintiffs' GET, POST and GIF submissions are excepted from §2701(c)(2) because they are "intended for" the DoubleClick-affiliated Web sites who have authorized

DoubleClick's access. The cookie identification numbers sent to DoubleClick from plaintiffs' computers fall outside of Title II's protection because they are not in "electronic storage" and, even if they were, DoubleClick is authorized to access its own communications.

In light of the above findings, we rule that all of plaintiffs' communications accessed by DoubleClick fall under §2701(c)(2)'s exception or outside Title II and, accordingly, are not actionable. Therefore, plaintiffs' claim under the Title II (Claim I) is dismissed.

Claim II. Wiretap Act

Plaintiffs' second claim is that DoubleClick violated the Federal Wiretap Act ("Wiretap Act"), 18 U.S.C. §2510, et. seq.. The Wiretap Act provides for criminal punishment and a private right of action against:[22]

[22] 18 U.S.C. §2520 confers a private right of action to persons injured by violations of the Wiretap Act.

> "any person who--(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept wire, oral, or electronic communication [except as provided in the statute]." 18 U.S.C. §2511.

For the purposes of this motion, DoubleClick concedes that its conduct, as pled, violates this prohibition. However, DoubleClick claims that its actions fall under an explicit statutory exception:

> "It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception <u>unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or any State</u>." 18 U.S.C. §2511(2)(d) ("§2511(2)(d)") (emphasis added).

DoubleClick argues once again that the DoubleClick-affiliated Web sites have consented to its interceptions and, accordingly, that its conduct is exempted from the Wiretap Act's general prohibition as it was from the Title II's. Plaintiffs deny that the Web sites have consented and argue that even if the Web sites do consent, the exception does not apply because DoubleClick's purpose is to commit "criminal or tortious act[s]."

As a preliminary matter, we find that the DoubleClick-affiliated Web sites are "parties to the communication[s]" from plaintiffs and have given sufficient consent to DoubleClick to

intercept them. In reviewing the case law and legislative histories of Title II and the Wiretap Act, we can find no difference in their definitions of "user" (Title II) and "parties to the communication" (Wiretap Act) or "authorize" (Title II) and "consent" (Wiretap Act)[23] that would make our analysis of the Web sites' consent under Title II inapplicable to the Wiretap Act. See discussion supra Section I(C). Therefore, the issue before us is: assuming that DoubleClick committed every act alleged in the Amended Complaint, could this evince a "criminal or tortious" purpose on DoubleClick's part?

In light of the DoubleClick-affiliated Web sites' consent, plaintiffs must allege "either (1) that the primary motivation, or (2) that a determinative factor in the actor's [DoubleClick's] motivation for intercepting the conversation was to commit a criminal [or] tortious... act." United States v. Dale, 991 F.2d 819, 841-42 (D.C. Cir. 1993), cert. denied 510 U.S. 1030 (1993) (quoting United States v. Vest, 639 F.Supp. 899, 904 (D. Mass. 1986), aff'd, 813 F.2d 477 (1st Cir. 1987)). However, in reviewing the sufficiency of plaintiffs' allegations, we bear in

---

[23] Indeed, courts have emphasized that "consent" must be construed broadly under the Wiretap Act. See United States v. Amen, 831 F.2d 373, 378 (2d Cir. 1987)("Congress intended the consent requirement to be construed broadly."); Griggs-Ryan v. Smith, 904 F.2d 112, 116 (1st Cir. 1990) (citing United States v. Willoughby, 860 F.2d 15, 19 (2d Cir. 1988)).

mind that the mere existence of [a] lawful purpose alone does not "sanitize a[n interception] that was also made for an illegitimate purpose." Sussman v. ABC, 186 F.3d 1200, 1202 (9th Cir. 1999), cert denied, 528 U.S. 1131 (2000).

Section 2511(2)(d)'s legislative history and caselaw make clear that the "criminal" or "tortious" purpose requirement is to be construed narrowly, covering only acts accompanied by a specific contemporary intention to commit a crime or tort. The Wiretap Act originally exempted from its prohibition any interception of a wire or oral communication where one of the parties to the communication consented. See 2 U.S.Code Cong. & Ad.News, 90th Cong., 2d Sess., p. 2182 (1968).[24] However, Senator Phillip Hart objected that the exemption was too permissive because it conceivably allowed a party to intercept a communication for the purpose of breaking the law and injuring others. He feared that parties would use secret recordings for "insidious purposes such as blackmail, stealing business secrets, or other criminal or tortious acts in violation of Federal or State laws." Id. at 2236. Senators Hart and McClellan proposed an amendment to narrow the exemption to acts with "criminal,

[24] The original language read: "It shall not be unlawful under this Chapter for a party to any wire or oral communication, or a person given prior authority by a party to this communication to intercept such communication." S. Rep. No. 90-1097 (1968) at 12.

tortious or injurious" purposes, part of which was enacted as §2511(2)(d). The key distinction Senator Hart suggested should distinguish permissible from impermissible one-party consent recordings by private citizens was whether the defendant's intent in recording was to injure another party.[25] Compare 114 Cong.Rec. 14694-14695 (May 23, 1968) ("Such one-party consent is also prohibited when the party acts in any way with an intent to injure the other party to the conversation in any other way... For example, ...for the purpose of blackmailing the other party, threatening him, or publicly embarrassing him") with S. Rep. No. 90-1097 (1968) at 2236-37 ("There are, of course, certain situations in which consensual electronic surveillances may be used for legitimate purposes... [as with recordings made] without intending in any way to harm the nonconsenting party.")(emphasis added). Thus, the legislative record suggests that the element of "tortious" or "criminal" *mens rea* is required to establish a prohibited purpose under §2511(2)(d).

Plaintiffs attempt to meet §2511(2)(d)'s "purpose" requirement by arguing that their six non-Wiretap Act claims against DoubleClick "plead conduct that has underlying it a

---

[25] As a basic rule of interpreting legislative history, "[the] explanation of the sponsor of the [statutory] language, is an 'authoritative guide to the statute's construction." Bowsher v. Merck & Co., Inc., 460 U.S. 824, 832-33 (1983)(citing North Haven Board of Educ. v. Bell, 456 U.S. 512, 527 (1982).

tortious purpose and/or that translates into tortious acts." Plaintiffs' Brief at 16. In other words, by virtue of its tortious acts, DoubleClick must have had a tortious purpose.

Courts applying §2511(2)(d) have consistently ruled that a plaintiff cannot establish that a defendant acted with a "criminal or tortious" purpose simply by proving that the defendant committed any tort or crime. Recently, in Sussman v. ABC, 186 F.3d 1200 (9th Cir. 1999) (Kozisnki, J.), the Ninth Circuit addressed a case in which a plaintiff sued the American Broadcasting Companies, Inc. ("ABC") under the Wiretap Act. The plaintiff argued that ABC could not avail itself of §2511(2)(d) because the recording violated state privacy law and, therefore, ABC's purpose was "tortious." Judge Kozinski, writing for a unanimous panel, rejected plaintiff's argument and dismissed the Wiretap Act claim, explaining,

> "[U]nder section 2511, 'the focus is not upon whether the interception itself violated another law; it is upon whether the purpose for interception--its intended use--was criminal or tortious...' [citations omitted] Where the purpose [of a taping] is not illegal or tortious, but the means are, the victims must seek redress elsewhere... Although ABC's taping may well have been a tortious invasion under state law, plaintiffs have produced no probative evidence that ABC had an illegal or tortious purpose when it made the tape." Id. at 1202.

The Ninth Circuit ruled similarly in Deteresa v. ABC, 121 F.3d 460 (9th Cir. 1997), holding, "Deteresa [plaintiff] contends that

‘Radziwill and ABC [defendants] were by the taping committing the aforesaid crimes and torts.’ This argument begs the question. For this claim to survive summary judgment, Deteresa had to come forward with evidence to show that Radziwill taped the conversation for the purpose of violating Cal.Penal Code § 632, for the purpose of invading her privacy, for the purpose of defrauding her, or for the purpose of committing unfair business practices. The record is devoid of any such evidence.” Id. at 467, n.4.

The Seventh Circuit and Sixth Circuit have reached the same conclusion. In another case involving ABC, J.H. Desnick v. ABC, 44 F.3d 1345, 1353 (1995)(Posner, J.), the Seventh Circuit dismissed plaintiffs’ CFAA claims because they failed to allege that defendants’ purpose was tortious. Like Judge Kozisnki, Judge Posner held for a unanimous panel that the commission of a tortious act did not prove a tortious purpose. He found that “[t]he defendants did not order the camera-armed testers into the Desnick Eye Center’s premises in order to commit a crime or tort. Maybe the program as it was eventually broadcast was tortious... But there is no suggestion that the defendants sent the testers into the Wisconsin and Illinois officers for the purpose of defaming plaintiffs... [defendants’ allegedly tortious act]”). Id. The Sixth Circuit similarly distinguished tortious conduct

from purpose based on *mens rea*, stating: "'It is the use of the interception with intent to harm rather than the fact of interception that is critical to liability....'" Boddie v. ABC, 881 F.2d 267, 270 (6th Cir. 1989)(emphasis added)(quoting By-Prod Corp. v. Armen-Berry Co., 668 F.2d 956, 960 (7th Cir. 1982).

A number of district courts have interpreted §2511(2)(d) in the same manner. See, e.g., Medical Lab. Mgmt. Consultants v. ABC, 30 F.Supp.2d 1182, 1205 (D. Ariz. 1998) ("[Plaintiffs] offer no support for the assertion that Defendants recorded the meeting for the purpose of committing a tort, which, as the statute indicates, is the proper focus of inquiry in a § 2511 claim. Even if Defendants were found liable for fraud, the question is not whether they are ultimately liable for conduct found to be tortious, but whether, at the time the recording took place, they recorded the conversation with the express intent of committing a tort."); U.S. v. Kolovas, 1998 WL 452218, *4 (D. Mass. July 27, 1998) ("Kolovas argues that because the recording itself was made in violation of state law, it was made for the purpose of violating state law. The superficial logic of this argument has been rejected by at least one court [citation omitted]... if state law were to render tortious conduct as defined by the very act of recording that Congress sought to permit, the provisions of §2511(d) would be rendered meaningless."); Roberts v. American

Intl., Inc., 883 F.Supp. 499, 503 (E.D.C.A. 1995) (finding no "tortious purpose" in case where "there is no evidence, nor even any allegations that [defendant's] purpose in tape recording her supervisor was either criminal or tortious outside any allegations of violation of the [state] privacy laws."); Payne v. Norwest Corp., 911 F.Supp. 1299, 1304 (D. Mont. 1995), aff'd in part, rev'd in part and remanded on other grounds, 206 F.3d 92; United States v. DiFelice, 837 F. Supp. 81, 82 (S.D.N.Y. 1993)("Assuming that [the challenged] recordings violated Massachusetts law, that fact by itself does not establish that he intercepted the conversations 'for the purpose of committing [a] criminal or tortious act...'").

Plaintiffs seek to distinguish the weight of these precedents from the instant case on the ground that the bulk of the above cases involved news gathering and that Congress and courts have excepted this conduct on First Amendment considerations. Specifically, they point the 1986 amendment of §2511(2)(d), in which Congress reacted to a Sixth Circuit decision, Boddie v. American Broadcasting Cos., 731 F.2d 333 (6th Cir. 1984). When the Sixth Circuit decided Boddie, §2511(2)(d)'s one-party consent exception did not apply to interceptions for the purpose of committing any "criminal, tortious, or other injurious act" (emphasis added). In Boddie, the Sixth Circuit

ruled that the clause “other injurious act[s]” could provide a basis for holding defendants civilly liable, even when they had violated no civil or criminal law. Id. at 339. Congress worried that Boddie’s broad interpretation of “injurious” could facilitate "attempts by parties to chill the exercise of First Amendment rights through the use of civil remedies under [the Wiretap Act].” S. Rep. No. 99-541, at 17 (1986) (Congress emphasized that it did not want §2511(2)(d) to be “a stumbling block in the path" of investigative journalists who record conversations). In response, it removed "injurious" from section §2511(2)(d). Thus, the legislative history supports the contention that Congress struck “injurious” conduct from §2511(2)(d)’s one-party consent exception partly out of concern for the press. See Medical Lab. Mgmt. Consultants, 30 F.Supp.2d 1182, 1205-06 (discussing legislative history of §2511(2)(d) and Congress’ concern with protecting the media); Scott Golde, Media Organizations' Exposure to Liability Under the Federal Wiretapping Act: The Medical Laboratory Management Consultants Case, 76 Wash.U.L.Q. 431, 435 (1998).

However, plaintiffs overreach when they argue that Congress and the courts created a general rule that “tortious purpose” exists wherever an intentional action is later determined to have constituted a tort, save when journalism is involved. Although

Congress deleted "injurious" purpose from §2511(2)(d) partly out of concern for press freedom, it in no way indicated that the press enjoyed special standing under the remaining terms of §2511(2)(d). Had Congress wished to confer special protection on the press, it could have done so explicitly. Courts interpreting §2511(2)(d) have drawn no distinction between media defendants and the general public. In cases involving media defendants, they have consistently grounded their demand for specific contemporary tortious or criminal purpose in §2511(2)(d)'s general language and legislative history, not in an exception for the media. See Sussman v. ABC, 186 F.3d at 1202 ("If the district court interpreted section 2511 as containing a blanket exemption for journalists, we cannot agree. Congress could have drafted the statute so as to exempt all journalists from its coverage, but did not. Instead, it treated journalists just like any other party who tapes conversations surreptitiously.")(emphasis added); J.H. Desnick v. ABC, 44 F.3d at 1353 (analysis did not rely on fact that recording was made for investigative reporting, only that its purpose was non-tortious)"; Deteresa v. ABC, 121 F.3d 460, 467, n.4 (analysis underlying finding that ABC did not violate §2511(2)(d) because it had no 'tortious purpose,' in no way distinguished between media and non-media defendants). And in suits not involving

journalism, courts have demanded evidence of the same tortious or criminal purpose. See, e.g., Roberts v. American Intl., Inc., 883 F.Supp. at 503 (finding no tortious purpose for recording in a employment discrimination action because "[t]he facts do not show at this point that [plaintiff] tape recorded to extort or blackmail her supervisor or company, nor do the facts presently show that she engaged in tape recording to cause emotional distress."); U.S. v. Kolovas, 1998 WL 452218 at *4 (criminal case with no media party involved); United States v. DiFelice, 837 F. Supp. at 82 (criminal case with no media party involved); see also, Thomas v. Pearl, 998 F.2d 447, 451 (7th Cir. 1993) (in civil suit between basketball player and coach, Seventh Circuit held that "[Plaintiff] must show that [defendant] either intended to break the law or commit a tort against him in order to prove a violation of the federal statute.").

In the instant case, plaintiffs clearly allege that DoubleClick has committed a number of torts. However, nowhere have they alleged that DoubleClick's "primary motivation" or a "determining factor" in its actions has been to injure plaintiffs tortiously. The Amended Complaint does not articulate any facts that could support an inference that DoubleClick accessed plaintiffs' electronic communications with the "insidious" intent to harm plaintiffs or others. In fact, everything in the Amended

Complaint suggests that DoubleClick has been consciously and purposefully executing a highly-publicized market-financed business model in pursuit of commercial gain –- a goal courts have found permissible under §2511(2)(d).[26] Its technology and business strategy have been described, and indeed promoted, in the company's Security and Exchange Commission ("SEC") filings[27] and have been the focus of numerous articles in prominent periodicals and newspapers.[28] Indeed, the intricate details of

---

[26] See Berger v. Cable New Network, Inc., No. 94-46-VLG-JDS, 1996 WL 390528, at *3 (D. Mont. Feb. 26, 1996) ("[§2511(2)(d)] does not apply because this Court does not find that defendants made the recordings for the purpose of committing a crime or tortious act. Instead, the recordings were made for the purpose of producing a news story and for the defendants' commercial gain."), aff'd in part, rev'd in part, 129 F.3d 505 (9th Cir. 1997), vacated and remanded, 526 U.S. 808 (1999), aff'd in relevant part, 188 F.3d 1155 (9th Cir. 1999); see also Russell v. ABC, No. 94 C 5678, 1995 U.S.Dist.LEXIS 7528, at *4 (N.D.Ill. May 30, 1995)(citing, Desnick v. ABC, Inc., 44 F.3d at 1353-54).

[27] See, e.g.,; DoubleClick, Inc., 10-K SEC filing (Dec. 31, 1999) at 4-5; DoubleClick, Inc., 10-K (Dec. 31, 1998) at 1-2, 6; DoubleClick, Inc., S-1 SEC filing (Dec. 16, 1997) at 3-4.

[28] Media attention to privacy concerns with DoubleClick's technology pre-dated the instant lawsuit. See, e.g., Rachel Scheier, Internet privacy concerns DoubleClick's increasing power to compile info on Web users at issue, New York Daily News, January 27, 2000; Jennifer Tanaka, Getting Personal: Online shoppers will spend nearly $10 billion this holiday season. They'll surrender some of their privacy along with the cash, Newsweek, November 22, 1999; Robert O'Harrow Jr., Global Savvy Web 'Bug's' Impact on Privacy Draws Scrutiny Internet: Regulators are looking at stealth tool that tracks online users' activities and soon may be used to identify them by name, Los Angeles Times, November 15, 1999 at C2; Andrea Petersen and Jon G. Auerbach, Online Ad Titans Bet Big in Race to Trace Consumers' Web Tracks, Wall St. J., November 8, 1999 at B1; Leslie Miller and Elizabeth Weise, FTC studies 'profiling' by

each proprietary technology challenged by plaintiffs are public record in DoubleClick's patents. See, e.g., U.S. Patent No. 5,948,061 (issued September 7, 1999). DoubleClick's purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money by providing a valued service to commercial Web sites. If any of its practices ultimately prove tortious, then DoubleClick may be held liable for the resulting damage. However, a culpable mind does not accompany every tortious act. In light of the abundant evidence that DoubleClick's motivations have been licit and commercial and the utter lack of evidence that its intent has been tortious, we find as a matter of law that plaintiffs have failed to allege that DoubleClick has acted with a "tortious" purpose.

To summarize, we find that the DoubleClick-affiliated Web sites are "parties" to plaintiffs' intercepted communications under the Wiretap Act and that they consent to DoubleClick's interceptions. Furthermore, we find that plaintiffs have failed

---

Web sites, USA Today, November 8, 1999, at 1A; Leslie Walker, Time to Let the Cookies Crumble?, Washington Post, November 4, 1999 at E1; Hiawatha Bray, They're watching you ; More and more Web sites are tracking their users habits. Should you care?, The Boston Globe, February 11, 1999 at G6; Colin Beaven, They're watching you; Internet advertising tracking companies; includes a related article on Internet cookies, Esquire, August, 1997, No. 2, Vol. 128 at 104; Julia Angwin, Got Cookies?, S.F. Chron., March 11, 1997 at C4.

to allege that DoubleClick has intercepted plaintiffs' communications for a "criminal or tortious" purpose. Accordingly, we find that DoubleClick's actions are exempted from liability under the Wiretap Act by §2511(2)(d) and, thus, we dismiss Claim II.

Count III. Computer Fraud and Abuse Act

Plaintiffs' final federal claim is under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. §1030, et. seq. ("§1030") The CFAA provides:

> "[18 U.S.C. §1030](a) – whoever... (2)(c) intentionally accesses a computer without authorization, or exceeds authorized access, and thereby obtains... information from any protected computer if the conduct involved an interstate or foreign communication... shall be punished as provided in subsection (c) of this section.""

The CFAA also provides a civil right of action for victims under 18 U.S.C. §1030(g) ("§1030(g)"):

> "(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. Damages

> for violations involving damage as defined in section (e)(8)(A) are limited to economic damages..."

However, section 18 U.S.C. §1030(e)(8) ("§1030(e)(8)") limits the "damage" civilly recoverable to the following instances:

> "(e)(8) the term 'damage' means any impairment to the integrity or availability of data, a program, a system, or information that – (A) <u>causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals</u>; [B. Impairs medical care; C. Causes physical injury; D. Threatens public health or safety]." (emphasis added).

For the purposes of this motion, DoubleClick does not contest that plaintiffs' computers were "protected" under the CFAA or that its access was unauthorized. Instead, it claims that §1030(e)(8) creates a $5,000 damages threshold for each individual class member and that plaintiffs have failed to plead these damages adequately. Plaintiffs argue that "loss" under §1030(g) is distinct from "damage" and, accordingly, is not subject to §1030(e)(8)'s damage threshold. In the alternative, if §1030(e)(8)'s damage threshold is found applicable to plaintiffs' claims, plaintiffs argue that they easily meet the threshold by "aggregating" losses for the entire class over "any 1-year period."

A. <u>"Loss" pled under 18 U.S.C. §1030(g) is subject to §1030(e)(8)'s $5,000 statutory minimum damages.</u>

The first issue is whether "loss" pled under §1030(g) is subject to §1030(e)(8)'s $5,000 statutory minimum damages -- a question of statutory interpretation. The Supreme Court recently reviewed the basic canons of statutory interpretation in Robinson v. Shell Oil Co., 519 U.S. 337, 340-41 (1997). It explained:

> "Our first step in interpreting a statute is to determine whether the language at issue has a plain and unambiguous meaning with regard to the particular dispute in the case. Our inquiry must cease if the statutory language is unambiguous and 'the statutory scheme is coherent and consistent.' [citations omitted]. The plainness or ambiguity of statutory language is determined by reference to the language itself, the specific context in which that language is used, and the broader context of the statute as a whole."

See Washington v. Schriver, 240 F.3d 101, 108 (2d Cir. Jan. 5, 2001). However, where a statute's language conveys no "plain and unambiguous meaning, it is deemed "ambiguous" and a court may look to "legislative history and other extrinsic material" in interpreting it. Oklahoma v. New Mexico, 501 U.S. 221, 235 n. 5 (1991)(citations omitted); see Washington, 240 F.3d at 108.

Sections 1030(g) and 1030(e)(8)(A)'s language concerning "loss" is plainly inconsistent. On its face, §1030(e)(8)(A)'s definition of "damage" explicitly includes "loss." See §1030(e)(8)(A) ("the term 'damage' means any impairment... that – (A) causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals")(emphasis added). In

order to find that “loss” under §1030(g) is not subject to the $5,000 “damage” threshold, one would have to accept that Congress created two definitions of “loss” -- one under §1030(g) that is not subject to §1030(e)(8)’s $5,000 threshold, and one under §1030(e)(8) that is clearly subject to the threshold –- without explicitly defining or differentiating either. In contrast, the statute gives a clear definition of “damage” in §1030(e)(8) to which it explicitly refers in §1030(g).

Nevertheless, a “cardinal principle of statutory construction [is] that we must 'give effect, if possible, to every clause and word of a statute,'" Williams v. Taylor, 529 U.S. 362, 404 (2000)(quoting United States v. Menasche, 348 U.S. 528, 538-39 (1955)) and this principle supports two arguments for reading “loss” outside of §10(e)(8)(A)’s exception. First, the fact that §1030(g) uses the word “loss” in addition to damage suggests that the words have different meanings. See United States v. Bernier, 954 F.2d 818, 819-20 (2d Cir. 1992) (in interpreting statutory clause "second or subsequent,” the Second Circuit ruled that “[w]hile it is conceivable that the word ‘subsequent’ is used as a synonym for the word ‘second’ in [the clause], the use of the connector ‘or’ (rather than ‘and’), and the absence of commas around the ‘or subsequent’ phrase, suggest that each word in the statute was meant to be different; hence

the use of different words.") Second, §1030(g) states that "[d]amages for violations involving damage as defined in subsection (e)(8)(A) are limited to economic damages." The fact that the statute chooses to limit this clause to "violations involving damage as defined in subsection (e)(8)(A)," suggests that it recognizes "damages" outside of subsection (e)(8)(A) as well. Otherwise, the limitation would be meaningless.

In light of the obvious facial contradictions, we find that the CFAA is ambiguous about whether "loss" pled under §1030(g) is subject to §1030(e)(8)'s $5,000 threshold. Accordingly, we turn to its legislative history for further guidance. The only explanation in the legislative record for why §1030(g) refers to both "damage" and "loss" is found in the 1996 Senate Report, S. Rep. No. 104-357 (1996). It stated:

> "The 1994 amendment [to §1030(g)] required both 'damage' and 'loss,' but it is not always clear what constitutes 'damage.' For example, intruders often alter existing log-on programs so that user passwords are copied to a file which the hackers can retrieve later. After retrieving the newly created password file, the intruder restores the altered log-on file to its original condition. Arguably, in such a situation, neither the computer nor its information is damaged. Nonetheless, this conduct allows the intruder to accumulate valid user passwords to the system, requires all system users to change their passwords, and requires the system administrator to devote resources to resecuring the system. Thus, although there is arguably no 'damage,' the victim does suffer 'loss.' <u>If the loss to the victim meets the required monetary threshold</u>, the conduct should be criminal, and the victim should be entitled to relief.

> The bill therefore defines 'damage' in new subsection 1030(e)(8), with a focus on the harm that the law seeks to prevent. As in the past, the term 'damage' will require either significant financial losses under section 1030(e)(8)(A), or potential impact on medical treatment under section 1030(e)(8)(B)... Under the bill, damages recoverable in civil actions by victims of computer abuse would be limited to economic losses for violations causing losses of $5,000 or more during any 1-year period." (emphasis added).

S. Rep. No. 104-357 seems to make clear that Congress intended the term "loss" to target remedial expenses borne by victims that could not properly be considered direct damage caused by a computer hacker. The term "loss" was not meant to except certain injuries from §1030(e)(8)(A)'s damages threshold.[29] Indeed, S.

---

[29] Senator Patrick Leahy, a sponsor of the ECPA in 1984, recently introduced a bill, the Enhancement of Privacy and Public Safety in Cyberspace Act, S. 3083, 106th Cong. (2000), in the Senate that expressly seeks to clarify (1) what constitutes "loss," and (2) that "loss" is subject to the $5,000 monetary threshold. See Cong. Rec. S8823, 106th Cong. (Sep. 20, 2000). The relevant of provision of that bill, is completely consistent with S. Rep. No. 104-357's explanation of "loss." It states:

"(10) the term `loss' includes--

`(A) the reasonable costs to any victim of--
`(i) responding to the offense;
`(ii) conducting a damage assessment; and
`(iii) restoring the system and data to their condition prior to the offense; and
`(B) any lost revenue or costs incurred by the victim as a result of interruption of service.';"

Prior Senate Report, S. Rep No. 101-544 (1990), further supports this conclusion. It explained that the proposed private right of action, later codified as §1030(g), "would create a civil cause of action for those who suffer violations of the Computer Fraud and Abuse Act. Plaintiffs would still have to meet the

Rep. No. 104-357's declaration that "If the loss to the victim meets the required monetary threshold, the conduct should be criminal, and the victim should be entitled to relief" (emphasis added), leaves no doubt but that "loss" under §1030(g) remains subject to §1030(e)(8)(A)'s $5,000 threshold. This reading is consistent with Congress' general intent to limit federal jurisdiction to cases of substantial computer crimes.[30]

[then] $1,000 threshold..." (emphasis added). It is noteworthy that the 1990 Report makes all injuries from CFAA "violations" subject to 1030(e)(8)(A)'s threshold, not just "damages." See also S. Rep. No. 99-432, at 2482-2483 ("the [Senate] Committee intends to make clear that losses caused by the same act may be aggregated for purposes of meeting the [then] $1,000 threshold.")(emphasis added); 132 Cong. Rec. S14453 (daily ed. Oct. 1, 1986)(statement of co-sponsor Sen. Trible) ("In addition, the concept of 'loss' embodied in this paragraph will not be limited solely to the cost of actual repairs. The Justice Department has suggested that other costs, including the cost of lost computer time necessitated while repairs are being made, be permitted to count toward the [then] $1,000 valuation. I and the other sponsors of this bill agree.").

[30] Senator Laxalt, one of the CFAA's sponsors, explained that the monetary threshold was meant, "first, to distinguish between alterations that should fairly be treated as misdemeanors and those that should be treated as felonies; and second, to limit federal jurisdiction to the felonious alterations. Setting a specific loss value is one way to achieve this end..." 132 Cong. Rec. S4072 (daily ed. Apr. 10, 1986)(statement of Sen. Laxalt regarding (a)(5))(emphasis added); see also 132 Cong. Rec. S14453 (daily ed. Oct. 1, 1986)(statement of co-sponsor Sen. Trible)("This bill will assert Federal jurisdiction over computer crimes only in those cases in which there is a compelling Federal interest. This reflects my belief and the Judiciary Committee's belief that the States can and should handle most such crimes, and that Federal jurisdiction in this area should be asserted narrowly."; see also Congr. Rec. S8823, 106th Cong. (Sep. 20, 2000)(Senator Leahy explaining that the damage threshold's purpose is to limit federal jurisdiction to

Caselaw further supports the conclusion that all injuries under §1030(g) are subject to §1030(e)(8)'s $5,000 threshold, whether termed "damage" or "loss." In Letscher v. Swiss Bank Corp., 1996 U.S. Dist. LEXIS 4908 (S.D.N.Y. April 16, 1996), Judge Sand dismissed a former employee's claim that his employer violated the CFAA by allegedly procuring his personal credit report without authorization. Letscher claimed that Swiss Bank's violation "caused him to 'invest[] his time, money, and talent requesting reports, making telephone calls, and writing letters causing him emotional distress and anguish.'" Id. at *7. The "time, money, [] talent, and [efforts]" for which Letscher sought compensation were clearly "losses" to him, not compensation for "damage" to the integrity of his data or computer. Nevertheless, Judge Sand held that Letscher's losses were still subject to §1030(e)(8)(A)'s $5,000 threshold and dismissed his claim finding that these losses were not "economic." Id.

In America Online, Inc. v. LCGM, 46 F. Supp. 2d 444, 451 (E.D.V.A. 1998), America Online, Inc. ("AOL") alleged that LCGM secretly collected AOL members' email addresses without AOL's authorization and then employed deceptive techniques to "spam" (i.e. to e-mail en masse) AOL members. The facts in AOL v. LCGM are quite similar to the hypothetical in S. Rep No. 101-544 that

---

major crimes).

illustrated the difference between “loss” and “damage” -– there was no “damage” to the function of AOL’s system or the data within it, only plaintiff’s “loss” from defendant’s trespass. Nonetheless, the court required a finding that AOL’s losses exceeded the “$5,000, the statutory threshold requirement” before it granted summary judgment. Id. at 450. Thus, it is clear that plaintiffs’ alleged injuries, whether described as “damage” or “loss,” are subject to §1030(e)(8)(A)’s $5,000 threshold.

B. Plaintiffs fail to allege facts that could support a finding that their injuries meet §1030(e)(8)(A)’s $5,000 threshold

Turning to the instant case, plaintiffs seek damages for their “‘loss’ - an invasion of their privacy, a trespass to their personal property, and the misappropriation of confidential data by DoubleClick... [as well the cost of the] affirmative steps [plaintiffs must take] to negate DoubleClick’s wrongful unauthorized access of their computers.” Plaintiffs’ Opposition Brief at 23. They argue that in determining whether plaintiffs have met §1030(e)(8)(A)’s $5,000 threshold, damages should be aggregated across all plaintiffs and all of DoubleClick’s acts for any given year.

1. Damages and losses under §1030(e)(8)(A) may only be aggregated across victims and time for a single act.

As a preliminary matter, we find that damages and losses under §1030(e)(8)(A) may only be aggregated across victims and over time for a single act. The relevant clause states that "the term 'damage' means any impairment to the integrity or availability of data, a program, a system, or information that – (A) causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals." The fact that §1030(e)(8)(A) is phrased in the singular ("any impairment to the integrity or availability of data, a program, a system, or information that--(a) causes loss"), rather than the plural (e.g., any impairments to the integrity or availability of data, programs, systems, or information that--(a) cause loss...), indicates that §1030(e)(8)(A) should only apply to single acts. The legislative history clarifies that this was Congress' intent. The Senate Judiciary Committee's report that accompanied the CFAA, Sen. R. No. 99-132, explains:

> "The Committee does not intend that every victim of acts proscribed under [1030(e)(8)(A)] must individually suffer a loss of [then] $1,000. Certain types of malicious mischief may cause smaller amounts of damage to numerous individuals, and thereby collectively create a loss of more than $1,000. By using 'one of more others'[31], the Committee intends to make clear that losses caused by the same act may be aggregated for the purposes of meeting the [then] $1,000 threshold." Id. at 5(emphasis added).

[31] The word "others" was replaced by "individuals" in the final bill.

This interpretation is consistent with Congress' overall intent to limit the CFAA to major crimes. See supra note 31. In contrast, plaintiffs cite no authority to support their reading of §1030(e)(8)(A). Therefore, we find that §1030(e)(8)(A) only allows aggregation of damage over victims and time for a single act.

2. Plaintiffs have failed to allege facts that could support a finding that plaintiffs suffered over $5,000 in damages and losses from any single act by DoubleClick.

In order to determine plaintiffs' damages and losses stemming from any single prohibited act by DoubleClick, we must first determine what constitutes a single act under §1030(e)(8)(A). Examining §1030(a)(2)(C), the relevant subsection, it is apparent that the definition of a prohibited act turns on the perpetrator's access to a particular computer. The prohibition is phrased in the singular: "[whoever] intentionally accesses a computer without authorization.. and thereby obtains... **(C)** information from any protected computer..." §1030(a)(2)(C) (emphasis added).[32] Thus, the

[32] We recognize that statute covers information "from any protected computer," meaning that a single act could involve information from multiple computers. For example, if someone accessed a White House computer and through that computer erased

suggestion that DoubleClick's accessing of cookies on millions of plaintiffs' computers could constitute a single act is refuted by the statute's plain language. Nevertheless, the statute is ambiguous about the scope of a single prohibited act on any one computer. One could reasonably argue from §1030(a)(2)(C)'s text that DoubleClick commits a violation each time it accesses a cookie on a plaintiff's hard drive. However, one could also plausibly maintain that DoubleClick's systematic uploading of data from a cookie on a particular computer's hard drive constitutes a single act of "access," even though it occurs over multiple electronic transactions. For the purposes of this motion, we need not choose between these two interpretations because even on the more liberal, plaintiffs fail to plead facts that could meet the damages threshold.

Plaintiffs essentially plead two bases of "damage or loss": (1) their cost in remedying their computers and data in the wake of DoubleClick's access, and (2) the economic value of their attention (to DoubleClick's advertisements) and demographic

---

information on State Department, Central Intelligence Agency, and FBI computers, the value of these damages and losses could be aggregated for the purposes of meeting §1030(e)(8)(A)'s damages threshold. However, in the instant case, DoubleClick individually accessed each plaintiff's computer and obtained no information through it from other computers.

information.[33] Clearly, any economic losses plaintiffs bore in securing or remedying their systems in the wake of DoubleClick's alleged CFAA violations would count towards §1030(e)(8)(A)'s damage threshold. See supra note 30 and accompanying text. However, as counsel demonstrated at oral argument, users may easily and at no cost prevent DoubleClick from collecting information by simply selecting options on their browsers or downloading an "opt-out" cookie from DoubleClick's Web site. See Transcript of February 22, 20001 Oral Argument at 15-18. Similarly, they have not pled that DoubleClick caused any damage whatsoever to plaintiffs' computers, systems or data that could require economic remedy. Thus, these remedial economic losses are insignificant if, indeed, they exist at all.

Plaintiffs also contend that they have suffered economic damages consisting of the value of: (1) the opportunity to present plaintiffs with advertising; and (2) the demographic information DoubleClick has collected. See Transcript of February 22, 20001 Oral Argument at 47, 54. Essentially, they

---

[33] Insofar as plaintiffs allege that they suffered emotional distress due to DoubleClick's "invasion of their privacy, [] trespass to their personal property, and [] misappropriation of confidential data," their injuries not actionable because only economic losses are recoverable under §1030(g). See Letscher, 1996 U.S. Dist. LEXIS 4908, at *7; see also S. Rep No. 101-544 (1990) ("Damages [under §1030(e)(8)(A)] are limited to economic damages, except for violations of the medical records section, when pain and suffering damages would be permitted.")

argue that because companies pay DoubleClick for plaintiffs' attention (to advertisements) and demographic information, the value of these services must, in some part, have rightfully belonged to plaintiffs. They point to AOL in which the court appeared to hold that damage to "reputation and goodwill" counted towards the damage threshold and argue that, by the same logic, the economic value of their attention and demographic information should count as well. See AOL, 46 F.Supp.2d at 451.

Even assuming that the economic value of plaintiffs' attention and demographic information could be counted towards the monetary threshold –- a dubious assumption[34] –- it would still be insufficient. We do not commonly believe that the economic value of our attention is unjustly taken from us when we choose to watch a television show or read a newspaper with advertisements and we are unaware of any statute or caselaw that holds it is. We see no reason why Web site advertising should be treated any differently. A person who chooses to visit a Web

[34] AOL, 46 F. Supp. 2d at 444, is unpersuasive on this point. Its reference to "reputation and goodwill" occurs in a one-line recitation of plaintiff's alleged bases for damages. The Virginia court offered no statutory, caselaw or legislative analysis to support its categorization of "reputation and goodwill" as economic damages in this context. In the absence of any discussion or authority to support its conclusion, AOL is unconvincing. In a broader sense, this type of damage seems far removed from the damage Congress sought to punish and remedy in the CFAA –- namely, damage to computer systems and electronic information by hackers.

page and is confronted by a targeted advertisement is no more deprived of his attention's economic value than are his off-line peers. Similarly, although demographic information is valued highly (as DoubleClick undoubtedly believed when it paid over one billion dollars for Abacus), the value of its collection has never been considered a economic loss to the subject. Demographic information is constantly collected on all consumers by marketers, mail-order catalogues and retailers.[35] However, we are unaware of any court that has held the value of this collected information constitutes damage to consumers or unjust enrichment to collectors. Therefore, it appears to us that plaintiffs have failed to state any facts that could support a finding of economic loss from DoubleClick's alleged violation of the CFAA.

Nevertheless, to the extent that some value could be placed on these losses, we find that the plaintiffs have failed to

---

[35] See, e.g., Jeff Sovern, Opting In, Opting Out, Or No Options At All: The Fight For Control Of Personal information, 74 Wash. L. Rev. 1033, 1036 (1999) ("The Direct Marketing Association, a trade association, estimates that more than 15,000 consumer mailing lists exist, containing some two billion names (including duplicates). More than 1000 commercial services are said to broker lists... Internet sites, and even Westlaw, have databases designed to locate individuals and to report on their transactions--including their bankruptcy records, lawsuits, liens, real property refinancings, and transfers--and the location of their assets. Other Internet sites list driver's license and motor vehicle information, and verify Social Security numbers.")(citations omitted).

allege facts that could support the inference that the damages and losses plaintiffs incurred from DoubleClick's access to any particular computer, over one year's time, could meet §1030(e)(8)(A)'s damage threshold. Accordingly, Count III of the Amended Complaint is dismissed.

Conclusion Concerning Federal Claims

Plaintiffs' Amended Complaint fails to plead violations of any of the three federal statutes under which they bring suit. The absence of evidence in the legislative or judicial history of any of these Acts to suggest that Congress intended to prohibit conduct like DoubleClick's supports this conclusion. To the contrary, the histories of these statutes reveal specific Congressional goals –- punishing destructive hacking, preventing wiretapping for criminal or tortious purposes, securing the operations of electronic communication service providers –- that are carefully embodied in these criminal statutes and their corresponding civil rights of action.

Furthermore, DoubleClick's practices and consumers' privacy concerns with them are not unknown to Congress. Indeed, Congress is currently considering legislation that specifically recognizes and regulates the online harvesting of user information. For

example, the "Consumer Internet Privacy Enhancement Act," H.R. 237, 107th Cong. (2001), now pending before a House Committee, imposes substantial notice and opt-out requirements on Web site operators who, unlike DoubleClick, compile personally identifiable information from users. See also, The Online Privacy protection Act of 2001, H.R. 89, 107th Cong. (2001); Electronic Privacy Protection Act, H.R. 112, 107th Cong. (2001); Social Security Online Privacy Protection Act, H.R. 91, 107th Cong. (2001); Consumer Privacy Protection Act, S. 2606, 106th Cong. (2000).[36] Although proposed legislation has no formal authoritative weight, it is evidence that Congress is aware of the conduct plaintiffs challenge and is sensitive to the privacy concerns it raises. Where Congress appears to have drawn the parameters of its regulation carefully and is actively engaged in the subject matter, we will not stray from its evident intent.

Counts IV - VII. Remaining State Claims

---

[36] Interestingly, some of these proposals seem to make exceptions for conduct like DoubleClick's. For example, H.R. 237 does not impose these requirements on Web sites that harvest non-personally-identifiable information –- a category into which DoubleClick falls –- and H.R. 112 explicitly excepts "cookies" from its scope of regulated data-harvesting technologies. See §2(e)(2)(B), H.R. 112, 107th Cong. (2001).

For the reasons set out above, we have dismissed plaintiffs' federal claims which were the sole predicate for federal jurisdiction. When federal claims are dismissed, retention of state law claims under supplemental jurisdiction is left to the discretion of the trial court. See 28 U.S.C. §1367(c)(3)(1994)("[d]istrict courts may decline to exercise supplemental jurisdiction over a claim... if... (3) the district court has dismissed all claims over which it has original jurisdiction."); Purgess v. Sharrock, 33 F.3d 134, 138 (2d Cir.1994); In re Merrill Lynch Ltd. P'ships Litig., 7 F. Supp. 2d 256, 258 (S.D.N.Y. 1997). We decline to exercise supplemental jurisdiction over plaintiffs' state law claims. Accordingly, the remaining counts of plaintiffs' Amended Complaint are dismissed as well.

CONCLUSION

For the foregoing reasons, defendant's motion to dismiss is granted and plaintiffs' Amended Complaint is dismissed with prejudice.[37]

IT IS SO ORDERED.

DATED: New York, New York
March 28, 2001

_____
NAOMI REICE BUCHWALD
UNITED STATES DISTRICT JUDGE

[37] Because dismissal on the pleadings constitutes a "terminat[ion]" under 28 U.S.C. §1407(a), the two cases transferred to this Court by the Judicial Panel on Multidistrict Litigation, Steinbeck v. DoubleClick, 00 Civ. 5705, C.A, N.O. 8:00-98 (C.D. Cal) and Freedman v. DoubleClick, 00 Civ. 7194, 2:00-1559 (E.D. La), need not be remanded. See Humphreys v. Tann, 487 F.2d 666 (6th Cir. 1973), cert denied, 416 U.S. 956 (1974); see also Lexecon Inc. v. Millberg Weiss Bershad Hynes & Lerach, 523 U.S. 26, 37 ("To be sure... the Panel is not meant to issue ceremonial remand orders in cases already concluded by summary judgment, say, or dismissal.").