November 8, 2005
Privacy 1: Privacy from commerce

- *In re GeoCities*, Federal Trade Commission (1999)
- *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001)
- Browse the TRUSTe website, <http://www.truste.org/>
- Jeri Clausing, *Privacy Watchdog Declines to Pursue Microsoft, a Backer*, *N.Y. Times*, March 22, 1999, <http://www.nytimes.com/library/tech/99/03/cyber/articles/23privacy.html>
- Joseph Reagle and Lorrie Faith Cranor, *The Platform for Privacy Preferences*, <http://www.w3.org/TR/NOTE-P3P-CACM/>
- *Code*, chapter 11

For further reading (optional):

- Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress* (May 2000), <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>
- Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193 (1998)
- James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors* (1997), <http://www.law.duke.edu/boylesite/foucault.htm>
- Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 Tex.L.Rev. 553 (1998), <http://reidenberg.home.sprynet.com/lex_informatica.pdf>

Computers are good at tracking and remembering, sorting and extracting. The ease of information collection has tended to shape our online privacy – or lack thereof. As Jerry Yang puts it:

> [I]magine the following two visits to a mall, one in real space, the other in cyberspace. In real space, you drive to a mall, walk up and down its corridors, peer into numerous shops, and stroll through corridors of inviting stores. Along the way, you buy an ice cream cone with cash. You walk into a bookstore and flip through a few magazines. Finally, you stop at a clothing store and buy a friend a silk scarf with a credit card. In this narrative, numerous persons interact with you and collect information along the way. For instance, while walking through the mall, fellow visitors visually collect information about you, if for no other reason than to avoid bumping into you. But such information is general - e.g., it does not pinpoint the geographical location and time of the sighting - is not in a format that can be processed by a computer, is not indexed to your name or another unique identifier, and is impermanent, residing in short-term human memory. You remain a barely noticed stranger. One important exception exists: The scarf purchase generates data that are detailed, computer-processable, indexed by name, and potentially permanent.
>
> By contrast, in cyberspace, the exception becomes the norm: Every interaction is

> like the credit card purchase. The best way to grasp this point is to take seriously, if only for a moment, the metaphor that cyberspace is an actual place, a computer-constructed world, a virtual reality. In this alternate universe, you are invisibly stamped with a bar code as soon as you venture outside your home. There are entities called "road providers," who supply the streets and ground you walk on, who track precisely where, when, and how fast you traverse the lands, in order to charge you for your wear on the infrastructure. As soon as you enter the cyber-mall's domain, the mall begins to track you through invisible scanners focused on your bar code. It automatically records which stores you visit, which windows you browse, in which order, and for how long. The specific stores collect even more detailed data when you enter their domain. For example, the cyber-bookstore notes which magazines you skimmed, recording which pages you have seen and for how long, and notes the pattern, if any, of your browsing. It notes that you picked up briefly a health magazine featuring an article on St. John's Wort, read for seven minutes a newsweekly detailing a politician's sex scandal, and flipped ever-so-quickly through a tabloid claiming that Elvis lives. Of course, whenever any item is actually purchased, the store, as well as the credit, debit, or virtual cash company that provides payment through cyberspace, takes careful notes of what you bought - in this case, a silk scarf, red, expensive.
>
> All these data generated in cyberspace are detailed, computer-processable, indexed to the individual, and permanent. While the mall example does not concern data that appear especially sensitive, the same extensive data collection takes place as we travel through other cyberspace domains - for instance: to research health issues and politics; to communicate to individuals, private institutions, and the state; and to pay our bills and manage our finances. Moreover, the data collected in these various domains can be aggregated to produce telling profiles of who we are, as revealed by what we do and say. The very technology that makes cyberspace possible also makes detailed, cumulative, invisible observation of our selves possible. One need only sift through the click-streams generated by our cyber-activity. The information we generate as a by-product of this activity is quite valuable. The private sector seeks to exploit it commercially, but individuals resist. Both sides lay powerful, clashing claims to this data generated in cyberspace. How we resolve this conflict warrants careful discussion.

Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193, 1198-99 (1998)

Unless you take specific steps to cover your tracks, browsing the web often means leaving a “clickstream” trail. Webservers log your computer’s Internet Protocol (IP) address with each web page request. They may set “cookies,” small identification files on your computer, to track browsing activity within and between web sessions. If you enter personally identifying information to make a purchase or enter a give-away, sites may be able to tie the browsing habits to you individually.

These technologies can work for us: Cookies and tracking enable Amazon to build "your store" around your past purchases and the likes of similar customers; they allow you to put an item into a virtual "shopping cart" to pay for later; they let you re-organize the news on the Google homepage.

With the added convenience come privacy concerns. Can the breadcrumbs we leave in our online travels be gathered to be used against us? Do those tracking us through cyberspace have our best interests in mind, or will they sell our profiles to advertisers, spam us with unwanted marketing, or use the information to charge us more for products we're predicted to need? Will the massive private databases become tempting targets for government subpoenas or third-party discovery requests, as well as for data-mining by those who collect information?

Currently, we address these privacy concerns with a grab-bag of law, code, and industry self-regulation (norms and markets). There is no comprehensive U.S. privacy law, instead privacy is protected through FTC regulation of "unfair or deceptive acts or practices"; private lawsuits for tort and contract; and claims under federal statute. Internet users engage in self-help by erasing browser cookies, installing pop-up blockers, or giving false information in web forms.

The Federal Trade Commission takes authority to oversee privacy practices from § 5 of the FTC Act (15 U.S.C. §§ 41-58, as amended). As the FTC describes:

> Under this Act, the Commission is empowered, among other things, to (a) prevent unfair methods of competition, and unfair or deceptive acts or practices in or affecting commerce; (b) seek monetary redress and other relief for conduct injurious to consumers; (c) prescribe trade regulation rules defining with specificity acts or practices that are unfair or deceptive, and establishing requirements designed to prevent such acts or practices; (d) conduct investigations relating to the organization, business, practices, and management of entities engaged in commerce; and (e) make reports and legislative recommendations to Congress.

The FTC complaint and settlement order in *In re Geocities* shows how this enforcement authority can be used.

In re Doubleclick, Inc. Privacy Litigation, by contrast, is a class action invoking federal computer crime and wiretap law. Read it not for the specific details of the federal laws (we'll cover those in more depth next week), but to see how poorly suited they can be to resolve consumer privacy concerns. As one example where they do reach, however, the First Circuit upheld a Wiretap Act indictment against a bookstore that offered email accounts to its customers, then intercepted email messages from Amazon to those users. *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2004):

> Defendant-appellee Bradford C. Councilman was Vice President of Interloc, Inc., which ran an online rare and out-of- print book listing service. As part of its service, Interloc gave book dealer customers an e-mail address at the domain

> "interloc.com" and acted as the e-mail provider. Councilman managed the e-mail service and the dealer subscription list.
>
> According to the indictment, in January 1998, Councilman directed Interloc employees to intercept and copy all incoming communications to subscriber dealers from Amazon.com, an Internet retailer that sells books and other products. Interloc's systems administrator modified the server's procmail recipe so that, before delivering any message from Amazon.com to the recipient's mailbox, procmail would copy the message and place the copy in a separate mailbox that Councilman could access. Thus, procmail would intercept and copy all incoming messages from Amazon.com before they were delivered to the recipient's mailbox, and therefore, before the intended recipient could read the message. This diversion intercepted thousands of messages, and Councilman and other Interloc employees routinely read the e-mail messages sent to Interloc subscribers in the hope of gaining a commercial advantage. … On July 11, 2001, a grand jury returned a two-count indictment against Councilman.

Finally, businesses too recognize they must respond to consumers' privacy concerns. Customers won't shop online if they are too afraid of having their data misused. Further, if the public raises a privacy outcry and companies fail to respond, the government may feel compelled to step in. To ward off government regulation, companies have stepped up with self-regulation through policies and through code.

On the policy side, most popular websites now post "privacy policies," describing the data they collect and their planned uses for it. Some ask third party clearinghouse TRUSTe to certify their practices. Browse the TRUSTe website, <http://www.truste.org/>, to see what certification entails. Does it reassure you about the practices of the sites where the seal appears?

P3P was an ambitious effort to take privacy policies beyond legal text to computer code. As proposed by the World-Wide Web Consortium (W3C), the "Platform for Privacy Preferences Project" provided a technical means for sites to describe their privacy practices. Users could configure their web browsers to accept or reject communications with sites based on whether the privacy policies met their preferences. Some of these features were included in IE6, but never reached widespread adoption. Read the W3C's P3P overview, <http://www.w3.org/TR/NOTE-P3P-CACM/>, to get a sense of how technology could make privacy law.

In re Geocities,
127 F.T.C. 94 (FTC Complaint and Order, Docket C-3850, 1999)

COMPLAINT
The Federal Trade Commission, having reason to believe that GeoCities, a corporation ("respondent"), has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent GeoCities is a California corporation with its principal office or place of business at 1918 Main Street, Suite 300, Santa Monica, California 90405.

2. Respondent has operated a World Wide Web ("Web") site located at http://www.geocities.com. This Web site is a virtual community consisting of consumers' personal home pages that are organized into 40 themed neighborhoods. Respondent "hosts" a personal home page by posting it to an address in the consumer's chosen neighborhood.

3. Respondent has provided numerous services including free and fee-based personal home pages, free e-mail service, contests and children's clubs. Respondent provides personal home pages and e-mail addresses to adults and children who reveal personal identifying and demographic information when they register with the Web site.

4. Respondent has more than 1.8 million members whom it refers to as "homesteaders." As of December 2, 1997, approximately 200,000 GeoCities homesteaders were between the ages of 3 and 15. As of May 18, 1998, approximately 50,000 homesteaders were under age 13. Respondent's site is one of the ten most frequently visited Web sites, and was the sixth top trafficked site in April 1998 with 14.1 million unique visitors ages 12 and up. Among visitors between the ages of 12 and 17, it was the third most frequently visited Web site in March 1998. One out of five U.S. Web users visited respondent's Web site in October 1997.

5. Respondent has created opportunities for third party advertisers to promote products in a targeted manner to its more than 1.8 million members through respondent's collection of personal identifying, demographic, and "special interest" information obtained in the registration process and through the placement of members' personal home pages in themed neighborhoods.

6. Respondent has derived its revenues from: selling third party advertising space on the Web site (including rotated ad banners, pop-up ads, and sponsorships of major areas on the Web site); selling personal identifying, demographic, and/or interest information collected from consumers who register; GeoPlus, an enhanced fee-based service that provides members extra server space for their personal home pages, among other benefits; merchandising in the Web site's GeoStore; and respondent's publishing unit (GeoPress Publishing).

7. Respondent has required consumers, including children, to complete a "New Member Application" form to become a GeoCities member. The form requests certain mandatory information and certain other information that respondent describes as 'optional." The form also asks consumers to designate whether they would like to receive "special offers" from a list of topics or from specific companies. The default setting on the form for special offers is for members to receive them unless members choose otherwise.

8. Respondent has promoted on its Web site a children's neighborhood called the "Enchanted Forest." The Enchanted Forest is designated as respondent's "KIDS" area, "[a] community for and by kids." To join the Enchanted Forest neighborhood, children must complete the New Member Application form and post personal home pages. As of May 18, 1998, there were approximately 40,300 homesteads in the Enchanted Forest neighborhood.

9. Respondent has promoted on its Web site a children's club in the Enchanted Forest neighborhood called the "GeoKidz Club." To join the GeoKidz Club, children must complete the "Official GeoCities GeoKidz Club Membership Request Form." This form requires applicants to be GeoCities members and to fill in all information requested, including name, age, e-mail address, GeoCities home page address, and gender. Respondent has also promoted on its Web site contests in the Enchanted Forest neighborhood for which children must complete the "Enchanted Forest Contest Entry Form," by providing their name, personal Web page address, and e-mail address.

10. Respondent has distributed a newsletter called the "World Report." The World Report is e-mailed at regular intervals to respondent's members and occasionally is posted on respondent's Web site. Members automatically receive the World Report but can discontinue receiving it by using respondent's "Profile Editor," a form used to revise members' registration information. The Profile Editor's default setting is for members to receive the World Report unless they request not to.

11. The acts and practices of respondent alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

DECEPTIVE PRACTICES IN CONNECTION WITH RESPONDENT'S COLLECTION AND USE OF PERSONAL IDENTIFYING INFORMATION

Misrepresentations involving information collection by GeoCities

12. Respondent has placed privacy statements on its New Member Application form [*Exhibit A*]. This form collects from consumers, including children, certain mandatory information (first and last name, zip code, e-mail address, gender, date of birth, and member name) and certain other information respondent designates as "optional" (education level, income, marital status, occupation, and interests). The form also asks consumers to designate whether they wish to receive "special offers" from advertisers, to

select from a list of special offer topics, and to designate whether they wish to receive specific products or services from individual companies. Respondent has also placed privacy statements on its "GeoCities Free Member E-mail Program" Web page [*Exhibit B*] and in the September 2, 1997 issue of the World Report newsletter [*Exhibit C*], which refer to consumers' information collected on the New Member Application form. Through the privacy statements in Exhibits A, B, and C, respondent has made the following statements about the uses and privacy of the information it collects:

A. "The following section is completely optional. We will not share this information with anyone without your permission, but will use it to gain a better understanding of who is visiting GeoCities. This information will help us to build a better GeoCities for everyone. . . . [The information requested is] Highest Level of Education Completed . . . Household Income . . . Marital Status . . . Occupation . . . Interests" [*Exhibit A*]

B. "When [consumers] apply to GeoCities we ask if they would like to receive information on a variety of topics. . . . Before we send anything out, we deliver an orientation e-mail to explain the program, to ensure that only those people who requested topically-oriented mail receive it and to protect your privacy. . . . We assure you this is a free service provided only to GeoCitizens who request this information, and we will NEVER give your information to anyone without your permission." [*Exhibit B*]

C. "[Certain e-mail to members] came from our friends at CMG Direct Corporation. It was only sent to homesteaders who clicked a box in the topic list on the GeoCities application. The letter was meant as a heads-up to those people that information about the interests they selected would be coming from reputable companies. . . . We are sorry about any confusion concerning these e-mails. We assure you that we will NEVER give your personal information to anyone without your permission." [*Exhibit C*]

13. Through the means described in Paragraph 12, respondent has represented, expressly or by implication, that the personal identifying information collected through its New Member Application form is used only for the purpose of providing to members the specific e-mail advertising offers and other products or services they request.

14. In truth and in fact, the personal identifying information collected through respondent's New Member Application form is not used only for the purpose of providing to members the specific e-mail advertising offers and other products or services they request. Respondent has also sold, rented, or otherwise marketed or disclosed this information, including information collected from children, to third parties who have used this information for purposes other than those for which members have given permission. For example, third parties have targeted unrequested e-mail advertising offers to individual members based on their chosen GeoCities neighborhoods. Therefore, the representation set forth in Paragraph 13 was, and is, false or misleading.

15. Through the means described in Paragraph 12, respondent has represented, expressly or by implication, that the "optional" information collected through its New Member

Application form is not disclosed to third parties without the consumer's permission, and is used only to gain a better understanding of who is visiting GeoCities.

16. In truth and in fact, respondent has disclosed the "optional" information it collects through the New Member Application form to third parties without the consumer's permission, and for purposes other than to gain a better understanding of who is visiting GeoCities. Respondent has disclosed this information, including information collected from children, to third parties who have used this information to target advertising to GeoCities' members. Therefore, the representation set forth in Paragraph 15 was, and is, false or misleading.

Misrepresentations involving sponsorship by GeoCities where information is collected by third parties

17. Respondent has disseminated or caused to be disseminated Enchanted Forest Web pages [*Exhibits D, H*]. These Web pages have promoted children's activities in the Enchanted Forest, including the Official GeoCities GeoKidz Club, through print [*Exhibit D*] and audio [*Exhibit E*] messages, and contests through print messages [*Exhibit H*]. Respondent has also disseminated or caused to be disseminated the July 16, 1997 issue of the World Report newsletter [*Exhibit F*], which also promotes the Official GeoCities GeoKidz Club. These promotions have caused children to reveal personal identifying information through the Official GeoCities GeoKidz Club Membership Request Form [*Exhibit G*] and the Enchanted Forest Contest Entry Form [*Exhibit I*]. Through its Web page and e-mail promotions, respondent has made the following statements:

A. "Welcome kids to this enchanting forest created by your friends for you to enjoy. . . . Join the GeoKidz Club at Enchanted Forest/3696 for fun and HTML help. Play Java games and be sure to visit Charlie, the GeoKidz Club's new dog." [*Exhibit E*]

B. "JOIN THE GEOKIDZ CLUB!

We all want a safe spot for our children to play and The GeoKidz Club is the perfect place. Enchanted Forest Community Leader Melange has been busy providing an HTML Center, games, message forums, a member's gallery and many more features for both parents and children to enjoy. The GeoKidz Club is always growing and expanding, so visit http://www.geocities.com/EnchantedForest/3696 often . . . and make sure to say hello to our virtual dog!" [*Exhibit F*]

C. "Join us in our quest to name our Prince and Princess, the mascots of Enchanted Forest! Enter the contest to name them by June 7th, and win 25 GeoPoints." (emphasis in original) [*Exhibit H*]

18. Through the means described in Paragraph 17, respondent has represented, expressly or by implication, that respondent collects and maintains the children's personal identifying information collected through the Official GeoCities GeoKidz Club Membership Request Form and Enchanted Forest Contest Entry Form.

19. In truth and in fact, respondent does not collect and maintain the children's personal identifying information collected through the Official GeoCities GeoKidz Club Membership Request Form and Enchanted Forest Contest Entry Form. In fact, the Official GeoCities GeoKidz Club and the GeoCities Enchanted Forest contests are run by third parties hosted on the GeoCities Web site, who collect the children's personal identifying information directly and maintain it. Therefore, the representation set forth in Paragraph 18 was, and is, false or misleading.

20. The acts and practices of respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this fifth day of February, 1999, has issued this complaint against respondents.

DECISION AND ORDER

DECISION AND ORDER

The Federal Trade Commission having initiated an investigation of certain acts and practices of the respondent named in the caption hereof, and the respondent having been furnished thereafter with a copy of a draft of complaint which the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge respondent with violation of the Federal Trade Commission Act; and

The respondent, its attorneys, and counsel for Federal Trade Commission having thereafter executed an agreement containing a consent order, an admission by the respondent of all the jurisdictional facts set forth in the aforesaid draft of complaint, a statement that the signing of said agreement is for settlement purposes only and does not constitute an admission by respondent that the law has been violated as alleged in such complaint, or that the facts as alleged in such complaint, other than jurisdictional facts, are true and waivers and other provisions as required by the Commission's Rules; and

The Commission having considered the matter and having determined that it had reason to believe that the respondent has violated the said Act, and that complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such agreement on the public record for a period of sixty (60) days, and having duly considered the comments filed thereafter by interested persons pursuant to § 2.34 of its Rules, now in further conformity with the procedure prescribed in § 2.34 of its Rules, the Commission hereby issues its complaint, makes the following jurisdictional findings and enters the following order:

1. Respondent GeoCities, is a corporation organized, existing, and doing business under and by virtue of the laws of the State of California, with its office or principal place of business located at 1918 Main Street, Suite 300, Santa Monica, California 90405.

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the respondent, and the proceeding is in the proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. "Child" or "children" shall mean a person of age twelve (12) or under.

2. "Parents" or "parental" shall mean a legal guardian, including, but not limited to, a biological or adoptive parent.

3. "Personal identifying information" shall include, but is not limited to, first and last name, home or other physical address (*e.g.*, school), e-mail address, telephone number, or any information that identifies a specific individual, or any information which when tied to the above becomes identifiable to a specific individual.

4. "Disclosure" or "disclosed to third party(ies)" shall mean (a) the release of information in personally identifiable form to any other individual, firm, or organization for any purpose or (b) making publicly available such information by any means including, but not limited to, public posting on or through home pages, pen pal services, e-mail services, message boards, or chat rooms.

5. "Clear(ly) and prominent(ly)" shall mean in a type size and location that are not obscured by any distracting elements and are sufficiently noticeable for an ordinary consumer to read and comprehend, and in a typeface that contrasts with the background against which it appears.

6. "Archived" database shall mean respondent's off-site "back-up" computer tapes containing member profile information and GeoCities Web site information.

7. "Electronically verifiable signature" shall mean a digital signature or other electronic means that ensures a valid consent by requiring: (1) authentication (guarantee that the message has come from the person who claims to have sent it); (2) integrity (proof that the message contents have not been altered, deliberately or accidentally, during transmission); and (3) non-repudiation (certainty that the sender of the message cannot later deny sending it).

8. "Express parental consent" shall mean a parent's affirmative agreement that is obtained by any of the following means: (1) a signed statement transmitted by postal mail or facsimile; (2) authorizing a charge to a credit card via a secure server; (3) e-mail accompanied by an electronically verifiable signature; (4) a procedure that is specifically authorized by statute, regulation, or guideline issued by the Commission; or (5) such

other procedure that ensures verified parental consent and ensures the identity of the parent, such as the use of a reliable certifying authority.

9. Unless otherwise specified, "respondent" shall mean GeoCities, its successors and assigns and its officers, agents, representatives, and employees.

10. "Commerce" shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

I.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with any online collection of personal identifying information from consumers, in or affecting commerce, shall not make any misrepresentation, in any manner, expressly or by implication, about its collection or use of such information from or about consumers, including, but not limited to, what information will be disclosed to third parties and how the information will be used.

II.

IT IS FURTHER ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with any online collection of personal identifying information from consumers, in or affecting commerce, shall not misrepresent, in any manner, expressly or by implication, the identity of the party collecting any such information or the sponsorship of any activity on its Web site.

III.

IT IS FURTHER ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the online collection of personal identifying information from children, in or affecting commerce, shall not collect personal identifying information from any child if respondent has actual knowledge that such child does not have his or her parent's permission to provide the information to respondent. Respondent shall not be deemed to have actual knowledge if the child has falsely represented that (s)he is not a child and respondent does not knowingly possess information that such representation is false.

IV.

IT IS FURTHER ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the online collection of personal identifying information, in or affecting commerce, shall provide clear and prominent notice to consumers, including the parents of children, with respect to respondent's practices with regard to its collection and use of personal identifying information. Such notice shall include, but is not limited to, disclosure of:

A. what information is being collected (*e.g.*, "name," "home address," "e-mail address," "age," "interests");

B. its intended use(s);

C. the third parties to whom it will be disclosed (*e.g.*, "advertisers of consumer products," mailing list companies," "the general public");

D. the consumer's ability to obtain access to or directly access such information and the means by which (s)he may do so;

E. the consumer's ability to remove directly or have the information removed from respondent's databases and the means by which (s)he may do so; and

F. the procedures to delete personal identifying information from respondent's databases and any limitations related to such deletion.

Such notice shall appear on the home page of respondent's Web site(s) and at each location on the site(s) at which such information is collected.

Provided that, respondent shall not be required to include the notice at the locations at which information is collected if such information is limited to tracking information and the collection of such information is described in the notice required by this Part.

Provided further that, for purposes of this Part, compliance with all of the following shall be deemed adequate notice: (a) placement of a clear and prominent hyperlink or button labeled **PRIVACY NOTICE** on the home page(s), which directly links to the privacy notice screen(s); (b) placement of the information required in this Part clearly and prominently on the privacy notice screen(s), followed on the same screen(s) with a button that must be clicked on to make it disappear; and (c) at each location on the site at which any personal identifying information is collected, placement of a clear and prominent hyperlink on the initial screen on which the collection takes place, which links directly to the privacy notice and which is accompanied by the following statement in bold typeface:

NOTICE: We collect personal information on this site. To learn more about how we use your information click here.

V.

IT IS FURTHER ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the online collection of personal identifying information from children, in or affecting commerce, shall maintain a procedure by which it obtains express parental consent prior to collecting and using such information.

Provided that, respondent may implement the following screening procedure that shall be deemed to be in compliance with this Part. Respondent shall collect and retain certain personal identifying information from a child, including birth date and the child's and parent's e-mail addresses (hereafter "screening information"), enabling respondent to identify the site visitor as a child and to block the child's attempt to register with respondent without express parental consent. If respondent elects to have the child register with it, respondent shall: (1) give notice to the child to have his/her parent provide express parental consent to register; and/or (2) send a notice to the parent's e-mail address for the purpose of obtaining express parental consent. The notice to the child or parent shall provide instructions for the parent to: (1) go to a specific URL on the Web site to receive information on respondent's practices regarding its collection and use of personal identifying information from children and (2) provide express parental consent for the collection and use of such information. Respondent's collection of screening information shall be by a manner that discourages children from providing personal identifying information in addition to the screening information. All personal identifying information collected from a child shall be held by respondent in a secure manner and shall not be used in any manner other than to effectuate the notice to the child or parent, or to block the child from further attempts to register or otherwise provide personal identifying information to respondent without express parental consent. The personal identifying information collected shall not be disclosed to any third party prior to the receipt of express parental consent. If express parental consent is not received by twenty (20) days after respondent's collection of the information from the child, respondent shall remove all such personal identifying information from its databases, except such screening information necessary to block the child from further attempts to register or otherwise provide personal identifying information to respondent without express parental consent.

VI.

Nothing in this order shall prohibit respondent from collecting personal identifying information from children or from using such information, as specifically permitted in the Children's Online Privacy Protection Act of 1998 (without regard to the effective date of the Act) or as such Act may hereafter be amended; regulations or guides promulgated by the Commission; or self-regulatory guidelines approved by the Commission pursuant to the Act.

VII.

IT IS FURTHER ORDERED that respondent GeoCities, and its successors and assigns, shall provide a reasonable means for consumers, including the parents of children, to obtain removal of their or their children's personal identifying information collected and retained by respondent and/or disclosed to third parties, prior to the date of service of this order, as follows:

A. Respondent shall provide a clear and prominent notice to each consumer over the age of twelve (12) from whom it collected personal identifying information and disclosed that

information to CMG Information Services, Inc., describing such consumer's options as stated in Part VII.C and the manner in which (s)he may exercise them.

B. Respondent shall provide a clear and prominent notice to the parent of each child from whom it collected personal identifying information prior to May 20, 1998, describing the parent's options as stated in Part VII.C and the manner in which (s)he may exercise them.

C. Respondent shall provide the notice within thirty (30) days after the date of service of this order by e-mail, postal mail, or facsimile. Notice to the parent of a child may be to the e-mail address of the parent and, if not known by respondent, to the e-mail address of the child. The notice shall include the following information:

1. the information that was collected (*e.g.*, "name," "home address," "e-mail address," "age," "interests"); its use(s) and/or intended use(s); and the third parties to whom it was or will be disclosed (*e.g.*, "advertisers of consumer products," "mailing list companies," "the general public") and with respect to children, that the child's personal identifying information may have been made public through various means, such as by publicly posting on the child's personal home page or disclosure by the child through the use of an e-mail account;

2. the consumer's and childs parents right to obtain access to such information and the means by which (s)he may do so;

3. the consumer's and childs parent's right to have the information removed from respondent's or a third party's databases and the means by which (s)he may do so;

4. a statement that childrens information will not be disclosed to third parties, including public posting, without express parental consent to the disclosure or public posting;

5. the means by which express parental consent may be communicated to the respondent permitting disclosure to third parties of a child's information; and

6. a statement that the failure of a consumer over the age of twelve (12) to request removal of the information from respondent's databases will be deemed as approval to its continued retention and/or disclosure to third parties by respondent.

D. Respondent shall provide to consumers, including the parents of children, a reasonable and secure means to request access to or directly access their or their childrens personal identifying information. Such means may include direct access through password protected personal profile, return e-mail bearing an electronically verifiable signature, postal mail, or facsimile.

E. Respondent shall provide to consumers, including the parents of children, a reasonable means to request removal of their or their childrens personal identifying information from respondent's and/or the applicable third party's databases or an assurance that such information has been removed. Such means may include e-mail, postal mail, or facsimile.

F. The failure of a consumer over the age of twelve (12) to request the actions specified above within twenty (20) days after his/her receipt of the notice required in Part VII.A shall be deemed to be consent to the information's continued retention and use by respondent and any third party.

G. Respondent shall provide to the parent of a child a reasonable means to communicate express parental consent to the retention and/or disclosure to third parties of his/her child's personal identifying information. Respondent shall not use any such information or disclose it to any third party unless and until it receives express parental consent.

H. If, in response to the notice required in Part VII.A, respondent has received a request by a consumer over the age of twelve (12) that respondent should remove from its databases the consumer's personal identifying information or has not received the express consent of a parent of a child to the continued retention and/or disclosure to third parties of a child's personal identifying information by respondent within twenty (20) days after the parent's receipt of the notice required in Part VII.B, respondent shall within ten (10) days:

1. Discontinue its retention and/or disclosure to third parties of such information, including but not limited to (a) removing from its databases all such information, (b) removing all personal home pages created by the child, and (c) terminating all e-mail accounts for the child; and

2. Contact all third parties to whom respondent has disclosed the information, requesting that they discontinue using or disclosing that information to other third parties, and remove the information from their databases.

With respect to any consumer over the age of twelve (12) or any parent of a child who has consented to respondent's continued retention and use of personal identifying information pursuant to this Part, such consumer's or parent's continuing right to obtain access to his/her or a child's personal identifying information or removal of such information from respondent's databases shall be as specified in the notice required by Part IV of this order.

I. Within thirty (30) days after the date of service of this order, respondent shall obtain from a responsible official of each third party to whom it has disclosed personal identifying information and from each GeoCities Community Leader a statement stating that (s)he has been advised of the terms of this order and of respondent's obligations under this Part, and that (s)he agrees, upon notification from respondent, to discontinue using or disclosing a consumer's or child's personal identifying information to other third parties and to remove any such information from its databases.

J. As may be permitted by law, respondent shall cease to do business with any third party that fails within thirty (30) days of the date of service of this order to provide the statement set forth in Part VII.I or whom respondent knows or has reason to know has failed at any time to (a) discontinue using or disclosing a child's personal identifying

information to other third parties, or (b) remove any such information from their databases. With respect to any GeoCities Community Leader, the respondent shall cease the Community Leader status of any person who fails to provide the statement set forth in Part VII.I or whom respondent knows or has reason to know has failed at any time to (a) discontinue using or disclosing a child's personal identifying information to other third parties, or (b) remove any such information from their databases.

For purposes of this Part: "third party(ies)" shall mean each GeoCities Community Leader, CMG Information Services, Inc., Surplus Software, Inc. (Surplus Direct/Egghead Computer), Sage Enterprises, Inc. (GeoPlanet/Planetall), Netopia, Inc. (Netopia), and InfoBeat/Mercury Mail (InfoBeat).

VIII.

IT IS FURTHER ORDERED that for the purposes of this order, respondent shall not be required to remove personal identifying information from its archived database if such information is retained solely for the purposes of Web site system maintenance, computer file back-up, to block a child's attempt to register with or otherwise provide personal identifying information to respondent without express parental consent, or to respond to requests for such information from law enforcement agencies or pursuant to judicial process. Except as necessary to respond to requests from law enforcement agencies or pursuant to judicial process, respondent shall not disclose to any third party any information retained in its archived database. In any notice required by this order, respondent shall include information, clearly and prominently, about its policies for retaining information in its archived database.

IX.

IT IS FURTHER ORDERED that for five (5) years after the date of this order, respondent GeoCities, and its successors and assigns, shall place a clear and prominent hyperlink within its privacy statement which states as follows in bold typeface:

NOTICE: Click here for important information about safe surfing from the Federal Trade Commission.

The hyperlink shall directly link to a hyperlink/URL to be provided to respondent by the Commission. The Commission may change the hyperlink/URL upon thirty (30) days prior written notice to respondent.

X.

IT IS FURTHER ORDERED that respondent GeoCities, and its successors and assigns, shall maintain and upon request make available to the Federal Trade Commission for inspection and copying the following:

A. For five (5) years after the last date of dissemination of a notice required by this order, a print or electronic copy in HTML format of all documents relating to compliance with Parts IV through IX of this order, including, but not limited to, a sample copy of every information collection form, Web page, screen, or document containing any representation regarding respondent's information collection and use practices, the notice required by Parts IV, V, and VII, any communication to third parties required by Part VII, and every Web page or screen linking to the Federal Trade Commission Web site. Each Web page copy shall be accompanied by the URL of the Web page where the material was posted online. Electronic copies shall include all text and graphics files, audio scripts, and other computer files used in presenting information on the World Wide Web; and

Provided that, after creation of any Web page or screen in compliance with this order, respondent shall not be required to retain a print or electronic copy of any amended Web page or screen to the extent that the amendment does not affect respondent's compliance obligations under this order.

B. For five (5) years after the last collection of personal identifying information from a child, all materials evidencing the express parental consent given to respondent.

XI.

IT IS FURTHER ORDERED that respondent GeoCities, and its successors and assigns, shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having responsibilities with respect to the subject matter of this order. Respondent shall deliver this order to current personnel within thirty (30) days after the date of service of this order, and to future personnel within thirty (30) days after the person assumes such position or responsibilities.

XII.

IT IS FURTHER ORDERED that respondent GeoCities, and its successors and assigns, shall establish an "information practices training program" for any employee or GeoCities Community Leader engaged in the collection or disclosure to third parties of consumers' personal identifying information. The program shall include training about respondent's privacy policies, information security procedures, and disciplinary procedures for violations of its privacy policies. Respondent shall provide each such current employee and GeoCities Community Leader with information practices training materials within thirty (30) days after the date of service of this order, and each such future employee or GeoCities Community Leader such materials and training within thirty (30) days after (s)he assumes his/her position or responsibilities.

XIII.

IT IS FURTHER ORDERED that respondent GeoCities, and its successors and assigns, shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. Provided, however, that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Part shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

XIV.

IT IS FURTHER ORDERED that respondent GeoCities, and its successors and assigns, shall, within sixty (60) days after service of this order, and at such other times as the Federal Trade Commission may require, file with the Commission a report, in writing, setting forth in detail the manner and form in which they have complied with this order.

XV.

This order will terminate on February 5, 2019, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

A. Any Part in this order that terminates in less than twenty (20) years;

B. This order's application to any respondent that is not named as a defendant in such complaint; and

C. This order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that the respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

CONCURRING STATEMENT OF COMMISSIONER ORSON SWINDLE

I have voted in favor of final issuance of the consent order in this matter because its provisions are appropriate to remedy the alleged violations of the law by GeoCities, Inc. However, I want to emphasize that my support for these provisions as a remedy for alleged law violations in this particular case does not necessarily mean that I would support imposing these requirements on other commercial Internet sites through either legislation or regulation.

In re DoubleClick Inc. Privacy Litig.
154 F. Supp. 2d 497 (S.D.N.Y. 2001)

NAOMI REICE BUCHWALD
UNITED STATES DISTRICT JUDGE

Plaintiffs bring this class action on behalf of themselves and all others similarly situated 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.

[FN 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."]

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

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.

…
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 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 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.

When users visit any of these DoubleClick-affiliated Web sites, a "cookie" is placed on their hard drives. 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." 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.

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. 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 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, 11. 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 on his screen when Lycos.com appears. The only objects missing are the banner advertisements; in their places lie blank spaces. The second part of the communication is an IP-address link to the DoubleClick server. 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.

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. 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.

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. Thus, if a user visits an unaffiliated Website, the DoubleClick cookie captures no information. Second, plaintiff does not allege that DoubleClick ever attempted to collect any 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.

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" target banner advertisements using these demographic 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, 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. 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 DoubleClick had already merged any of the information.

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 posted.

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. …

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 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 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.

…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:

> "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 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." 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) n23 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?

...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. ….

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). Its technology and business strategy have been described, and indeed promoted, in the company's Security and Exchange Commission ("SEC") filings and have been the focus of numerous articles in prominent periodicals and newspapers. Indeed, the intricate details of 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 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) causes loss aggregating at least $ 5,000 in value during any 1-year period to one or more individuals; [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. [**65] 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."

[P]laintiffs 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 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.

…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. n33 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. 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. 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. Essentially, they 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 -- 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 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.

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

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)("district 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.