Public Workshop on Online Profiling

Testimony of the Center for Democracy and Technology Before the Federal Trade Commission

November 30, 1999

Deirdre Mulligan

Staff Counsel

Introduction

The profiling techniques employed by online advertising networks raise troubling privacy concerns. Advertising networks are using unique identifiers to track and monitor individuals' online activities across multiple Web sites without their knowledge and consent. This practice undermines individuals' expectations of privacy by fundamentally changing the Web experience from one where consumers can browse and seek out information anonymously, to one where an individual's every move is recorded.

The profiling activities of advertising networks, such as DoubleClick which currently commands approximately 60% of market share, are the leading edge of a growing industry built upon the widespread tracking and monitoring of individuals' online behavior. The increasingly pervasive use of surreptitious monitoring systems breeds consumer distrust and undermines consumers' efforts to protect their privacy by depriving them of control over their personal information.

The practices of advertising networks have far-reaching impacts on consumers' online privacy. The advertising networks that engage in profiling are hidden from the individual. They reach through the Web site with whom the individual has chosen to interact with and, unbeknownst to the individual, extract information about the individual's activities. In the rare instances where individuals are aware of the fact that a third party is collecting information about them, they are unlikely to be aware that this information is being fed into a growing personal profile data mined[2] at a data warehouse[1] or that the data mined can be exercised

While several of the companies engaged in profiling state that they do not correlate information with identifying information such as name, e-mail, address, this does not on its own address the privacy concerns at issue. The highly detailed nature of the profiles and the capture of information that can be reasonably easily associated with a specific individual raise questions about the claims of anonymity and promises of non-identifiability. While the companies, in some instances, may not be using the information in identifiable form, the information may be quite capable of revealing the individual's identity, through the use of various computer tools and software.

Equally troubling is the possibility that any one of these companies might unilaterally decide to change its terms of service and retroactively attach identities to these extensive profiles -- contradicting the statement relied upon by consumers. We have seen Web

[1] A "data warehouse" is a system used for storing and delivering huge quan warehousing refers to the process used to extract and transform operational dat loading it into a central data store or "warehouse". Data warehousing allows to be consolidated and managed from a single database, which in turn allows and more "accurate" profiles more efficiently and less expensively.

[2] Data mining is "a set of automated techniques used to extract buried or information from large databases." (Ann CAVOUKIAN, Data Mining : Staking (Information and Privacy Commissioner of Ontario, Canada), http://www.ipc.on.ca/web_site.eng/matters/sum_pap/PAPERS/datamine.htm (last viewed on A successful data mining operation will make it possible to unearth patte afterwards, use the new information to make proactive knowledge-driven busines focuses on the automated discovery of new facts and relationships in data. Fo Thearling, From Data Mining to Database Marketing, Oct. 1995, wp9502.htm (last viewed on Oct. 17, 1999).

sites and online service providers attempt to change their privacy practices and terms of service. While some have come under heavy fire and stepped back, we are certain that many have gone unnoticed by consumers and advocates alike. A change in policy that so fundamentally alters the privacy expectation of consumers should not be permitted unless consumers have unequivocally consented.

As these companies merge with each other and with companies such as Abacus that maintain detailed personally identifiable profiles about individuals' offline activities, the consolidation of offline and online profiles will erode the distinction between online and offline identity. Online companies are aware of the sensitivity this raises. Consumers have shown an aversion to having their online activities tied to their identity.[3] Finally, recent revelations about government demands for access to individual profiles created in the consumer marketplace warn us that even the most benign information, such as grocery purchases, that provides insights into individuals' behavior are sought out by the government.

Perhaps most importantly, the profiles created by the advertising networks are being used to make decisions about specific individuals. While the name and e-mail address of the individual may remain obscure, the information the individual is able to access, the offers made to the individual are being determined by the business based on specific information collected about the individual. While the concern raised by the use of information about the individual to alter what information they see in the context of advertising may appear relatively trivial, this same practice, and perhaps data, can be used to make other decisions about the individual that even a privacy-skeptic may find objectionable. The info collected about the individual could be used to alter the prices at which goods or services, including important services such as life and health insurance, are offered, employed by a government, and could be used to alter the information viewed by individuals. While the impact of altered advertisements on the individual--harm ? benefit ?--can be disputed, these other examples indicate that there is a privacy interest in information about individuals actions and interactions when it is collected and used to make decisions about them.

Similar concerns, led CDT and other advocates to file a complaint asking the FTC to enjoin the shipment of the Intel Pentium III Processors equipped with unique identifiers.[4] Our complaint stated that the deployment of the Intel Pentium III Processors equipped with unique identifiers did not comport with concepts of privacy protection. We

---

[4] On February 26, 1999, the Center for Democracy and Technology (CDT), the Electronic Privacy Information Clearinghouse, and Consumer Action filed a Complaint and Request for relief with the Federal Trade Commission (FTC) seeking immediate action to prevent harm to consumer privacy from the pending deployment of the Intel Pentium III Processor Serial Number (PSN). Specifically, the complaint requested that the Commission enjoin the shipment of Intel Pentium III Processors equipped with PSN, and to enjoin computer manufacturers from shipping Pentium III PSN-equipped computers that are not turned "Off" in a secure manner. In addition to this specific and immediate relief, the complaint requested that the Commission commence an investigation into the privacy issues raised by the Intel Pentium III PSN, because we believe that a broader examination of the privacy implications of this and other computer and Internet-based identifiers is critically needed to ensure that consumer privacy is protected in the development and deployment of online authentication tools. Our complaint charged that the deployment of the PSN was a violation of individual privacy and, therefore, an unfair and deceptive trade practice under Section 5 of the FTC Act. The complaint charged that the impending release of the Intel Pentium III chip with an identifying serial number would harm consumers' privacy.

specifically noted that the PSN threatened consumer privacy by failing to provide consumers with effective notice of how data is handled and by facilitating the collection of personal information without consumers' consent -- two bedrock principles of fair information practice.

Like Intel, the profiling companies have recognized that their activity poses a threat to online privacy. And like Intel, their opening response to privacy concerns is inadequate.

We welcome the Federal Trade Commission and Department of Commerce's attention to the troubling practices explored during the Workshop and look forward to a swift resolution of the privacy concerns raised by online profiling.

I. What is online profiling ?

A. The practice and risks of profiling

"Profiling" is the collection of detailed data about an individual or a group of people (living in the same area or belonging to the same ethnicity for example). Profiling can be the compilation of information in a clearly identifiable fashion -- including information such as full name or social security number. It may be the collection of information about a unique individual without information about who that individual is -- DoubleClick's cookie card for example contains a profile of your trips but it does not contain any information about you. The term also includes the creation of a profile that does not contain information about a specific individual but is used to make decisions or impute traits to individuals who match this profile. For example, the widely condemned "racial profiling" does not use information about unique individuals, but rather imputes traits to individuals based on a characteristic.

"Online profiling" is when profiling captures the above activities when they occur on the Internet. A general description of the practices of the ad networks is : the practice of aggregating various data about Internet users' and consumers' preferences, interests, and transactions (purchases, sales,...), gathered primarily by tracking their movements online, and using the resulting profiles to create targeted advertising on Web sites. Profiling in the online environment can be split into a few categories. First, individual Web sites or online service providers can collect information from users -- both information provided by the individual and click stream or navigational data. This data may be captured for a limited duration -- session specific -- or may be collected and maintained as an ongoing portrait of the individual. It may be directly tied to a unique individual, to a pseudonym or to a specific, named individual.

With growing frequency, navigational and other data is being captured by third parties -- advertising networks or "profiling companies." With the permission of the Web site, but not the individual, these profiling companies place unique identifiers on individuals' computers. These identifiers are then used to track the individual as they surf the Web. The individual's profile grows with time, because online profiling is a continuing collection of his online behavior, despite the fact that the individual disconnects. The navigational data collected may include information such as, Web sites and Web pages visited, the time and duration of the visit, search terms typed in search engines' forms,

and other queries, purchases, "click through" responses to advertisements, and the previous page visited. In addition to long lists of collected information, a profile may contain "inferential" or "psychographic" data -- information that the business infers about the individual based on the behavioral data captured. From this amassed data, elaborate inferences may be drawn, including the individual's interests, habits, associations, and other traits[5]

B. How do online profiling companies capture data about individuals' online activities without their knowledge ?

To build profiles of individuals, online profiling companies want to create as complete a picture as possible of them. To do so, they capture various bits of information about individuals' online activities, for example the search terms people type in search engines' Web sites. It is certainly valuable for marketers and profilers to know what a Web user is seeking because it allows for advertisements to be designed to appeal to the individuals' particular interests. An ad-serving company like Double Click is capable of capturing all the search terms typed by every user of the famous Altavista search engine, with the ability to match these queries with a unique individual, and then use this information to accurately serve this individual with ad banners. To be accurate, it is more correct to say that it is only the computer that is targeted, since ad-serving companies use the information provided from a specific computer Here are some technical explanations.

1. When connecting to a search engine Web site

Let us take the example of a request on the Web site of Altavista (http://www.altavista.com):
When accessing the Altavista Web site, the user's browser sends information to the server:

- type of browser and operating system ;
- language(s) accepted by the browser (the Web user can select the language(s) in which he prefers to view Web pages. It is an optional feature on most browsers) ;
- TCP/IP address.

(This string of data is included in what is called the HTTP request[6]

The server hosting the Altavista Web site answers by transmitting the HTTP header and the source[7] HTML code of the Altavista[8] home page. Altavista also sends a "cookie" to the Web user's hard disk, with a unique identifier (in the example : AV_UID=db87527e16ecdb). Generally the user will be unaware that a cookie is being

[5] A psychographic study "joins consumers' measurable demographic characteristics aspects of attitudes, opinions and interests." Data mining specialists code and psychographic data from surveys, throw them together and analyze them u characteristics can be distinguished from all other groups. They can identify buy specific products and services by including questions relating to a product future intentions to purchase. Every kind of psychographic study adds the lifestyles to a demographic inquiry and uses quantitative survey techniques. Psychographics : Qu'est-Ce Que C'est ?, Marketing Tools, http://www.demographics.com/publications/mt/95_mt/9511 _mt/MT388.htm (last viewed 1999).

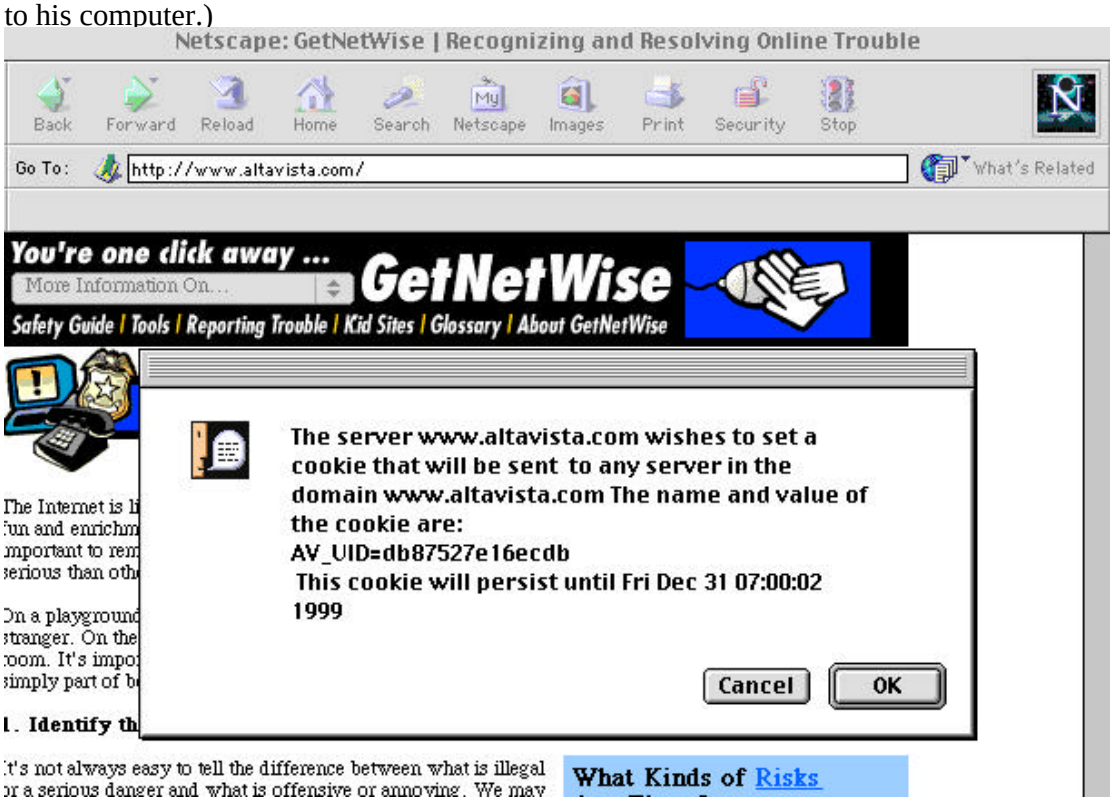
[6] HTTP stands for HyperText Transfer Protocol. For more information, see appendix.

[7] HTML stands for HyperText Markup Language.

[8] A cookie is a data file, in the form of a string of numbers and/or letters, that browser, and which can be used to track visitors as they move through the site.

set. If the Web user has activated the browser feature common in recent versions that warns of efforts to set cookies, the browser will display a user prompt (a window). It is important to note that, even if the browser is set to refuse cookies, this opposition mechanism only works in one direction. A user cannot configure her browser to prohibit "cookies" already on her computer from being requested and sent back to the domain who initially set it on the computer[9]

After clicking on OK or Cancel, to approve the request to set a cookie, the Altavista Web page is displayed. (If the Web user clicks on Cancel, the Altavista cookie will not be sent to his computer.)



In the HTML code the Web user's browser receives from Altavista, there is an invisible hyperlink to the DoubleClick Web site. The browser is triggered to send then an HTTP request to the DoubleClick Web site. Once again this request reveals information :

- type of browser and operating system ;
- DoubleClick's cookies stored on the Web user's hard disk (if the Web user has already visited Web sites belonging to the DoubleClick network[10]) ;

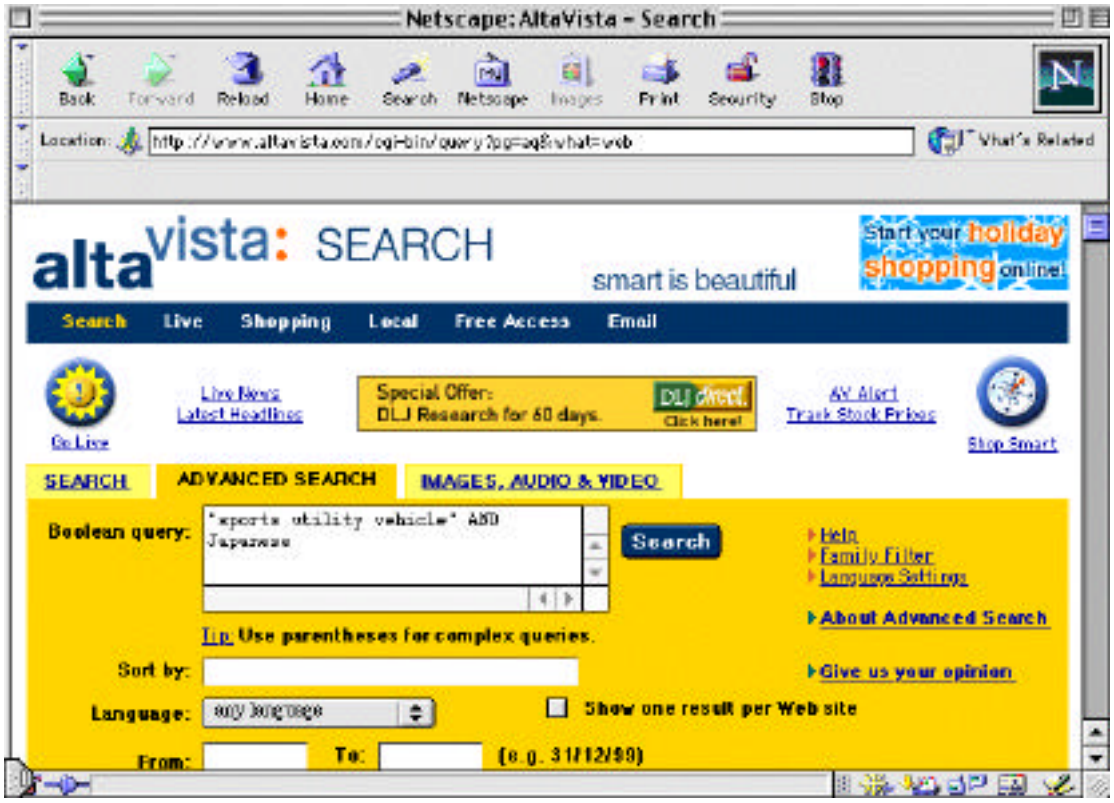
[9] Cf. Jean-Marc DINANT, Les traitements invisibles sur Internet, http://www.droit.fundp.ac.be/crid/eclip/luxembourg.html.

[10] The DoubleClick Network is a collection of about 1,500 Web sites delivering US News and World Report to Major League Baseball, Autobytel.com, FoodTV categories, such as business & finance, technology, travel, health, automotive. with DoubleClick an agreement to have the company serve ad banners on the for collecting and managing the data for advertising purposes. For http://www.doubleclick.net/annualreport/network.htm, and work/net_sites/us_network/default.htm.

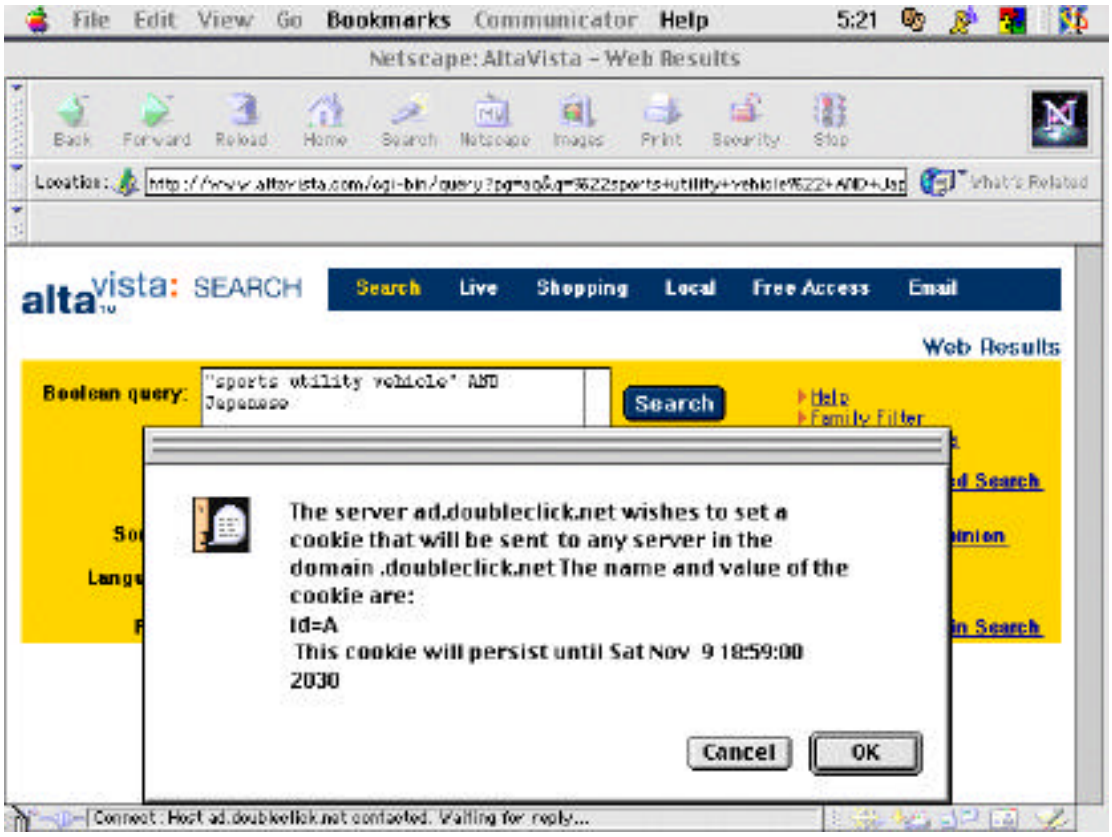
- language accepted by the browser (if communicated to the browser) ;
- the referrer, i.e. the address of the Web page visited by the Web user (in our example : http://www.altavista.com).

2. When searching

Let us imagine that the Web user wants to search for "sports utility vehicles" AND Japanese. (We went to the advanced search page of the Altavista Web site.)



When the user clicks on "Search", the browser sends this HTTP request to Altavista : http://www.altavista.com/cgi-bin/query?pg=aq&q=%22sports+utility+vehicle%22+AND+Japanese&r=&kl=XX&d0=&d1=&search.x=29&search.y=10



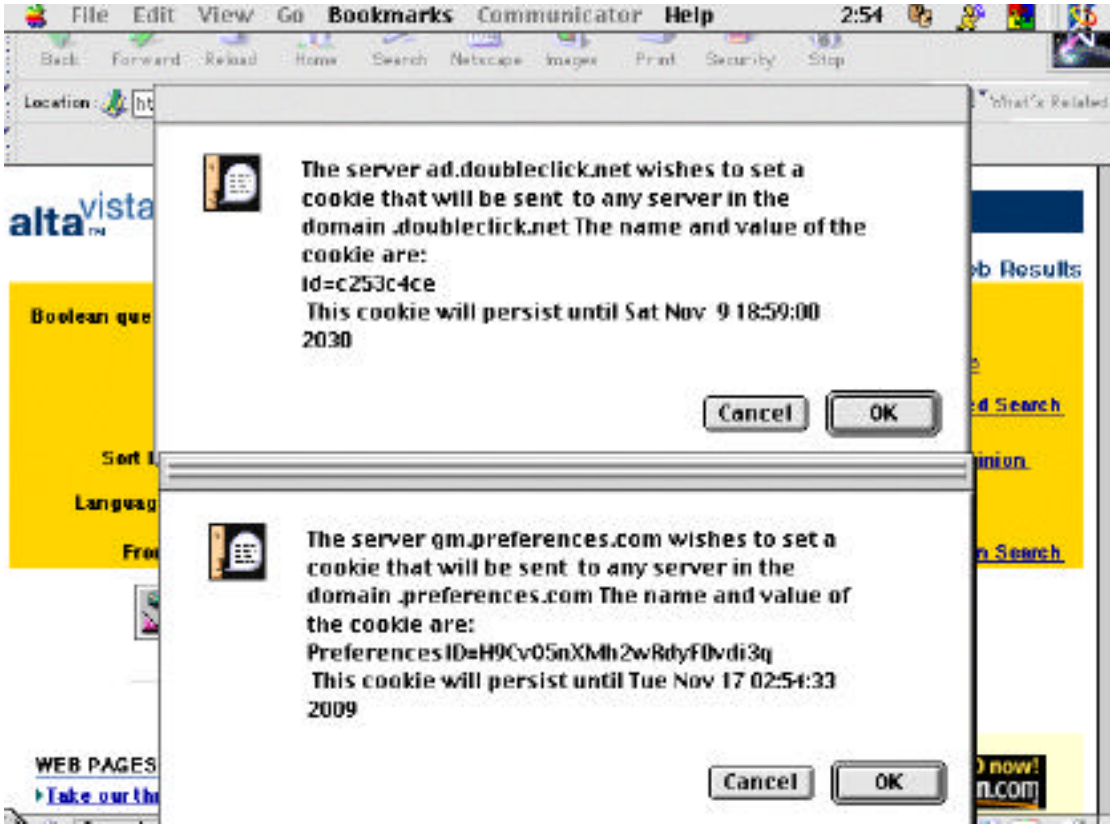
The HTML code of Altavista's answer contains an embedded image downloaded from DoubleClick's Web site. When displaying the Web Page, the browser sends an invisible request to DoubleClick's server, with the exact reference of the Web page that is being downloaded. In the HTTP header of the request, here is what appears :

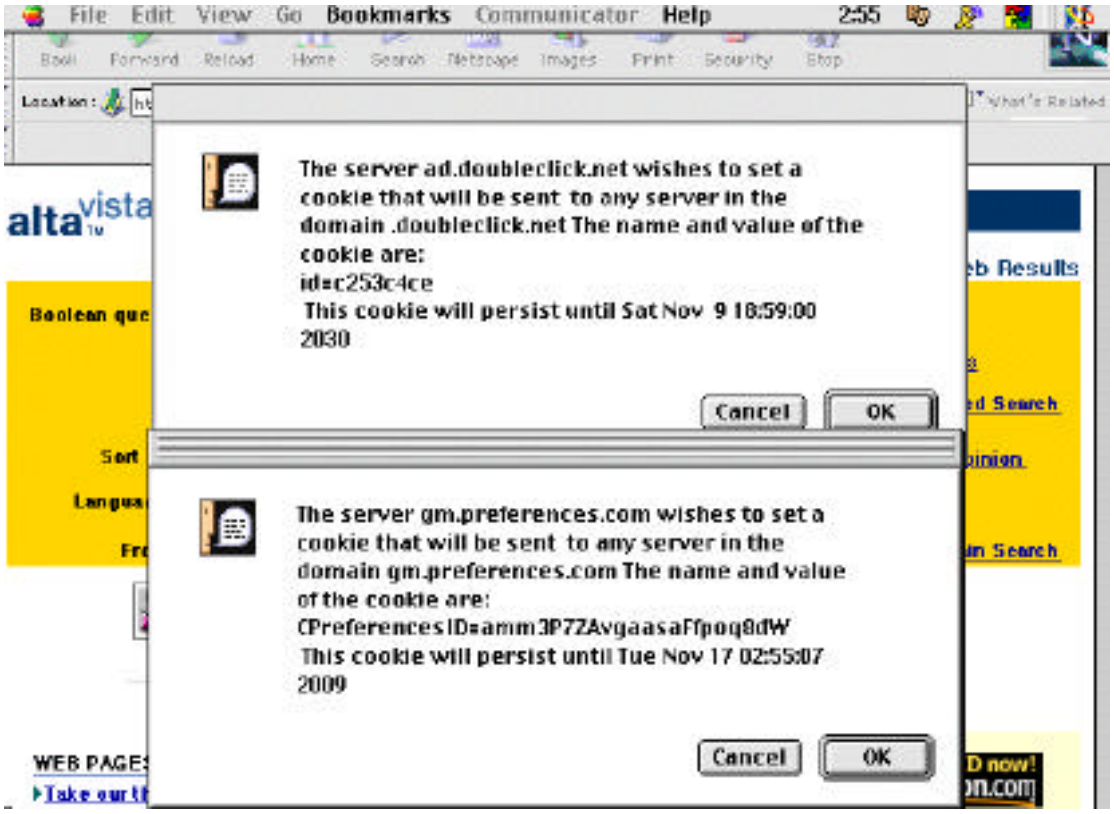
HTTP_REFERRER = http://www.altavista.com/cgi-bin/query?pg=aq&q=%22sports+utility+vehicle%22+AND+Japanese&r=&kl=XX&d0=&d1=&search.x=29&search.y=10

Before DoubleClick sends an ad banner, the company is aware of the search terms "sports utility vehicle" and Japanese. It enables DoubleClick to send a targeted ad to the Web user (in this case, an ad for General Motors cars, including sports utility vehicles). This ad banner is displayed at the same time as the results of the search request.

The General Motors' server also sends three cookies, one including a unique identifier, the two others adding some details to the Web user's profile,--probably some elements such as the search terms typed by the Web user (e.g., "sports utility vehicle"). (See the two next figures showing the DoubleClick's cookie and two of GM's cookies.)
Only if the browser has been configured to detect the sending of cookies in the HTTP header can the Web user notice that General Motors and DoubleClick are sending new cookies to his computer.

The cookies sent will sharpen the Web user's profile in DoubleClick and General Motors' databases.


File Edit View Go Bookmarks Communicator Help 2:54
Back Forward Reload Home Search Netscape Images Print Security Stop
Location:
alta vista
Boolean que
Sort
Languag
Fro
WEB PAGES
Take our th
b Results
d Search
inion
n Search
now!
n.com
The server ad.doubleclick.net wishes to set a cookie that will be sent to any server in the domain .doubleclick.net The name and value of the cookie are:
id=c253c4ce
This cookie will persist until Sat Nov 9 18:59:00 2030
Cancel
OK
The server gm.preferences.com wishes to set a cookie that will be sent to any server in the domain .preferences.com The name and value of the cookie are:
PreferencesID=H9Cv05nXMh2wRdyF0vdi3q
This cookie will persist until Tue Nov 17 02:54:33 2009
Cancel
OK



If we take a look at the cookies file on the hard disk, here is what has been downloaded so far (if the Web user has accepted all the cookies of course) :

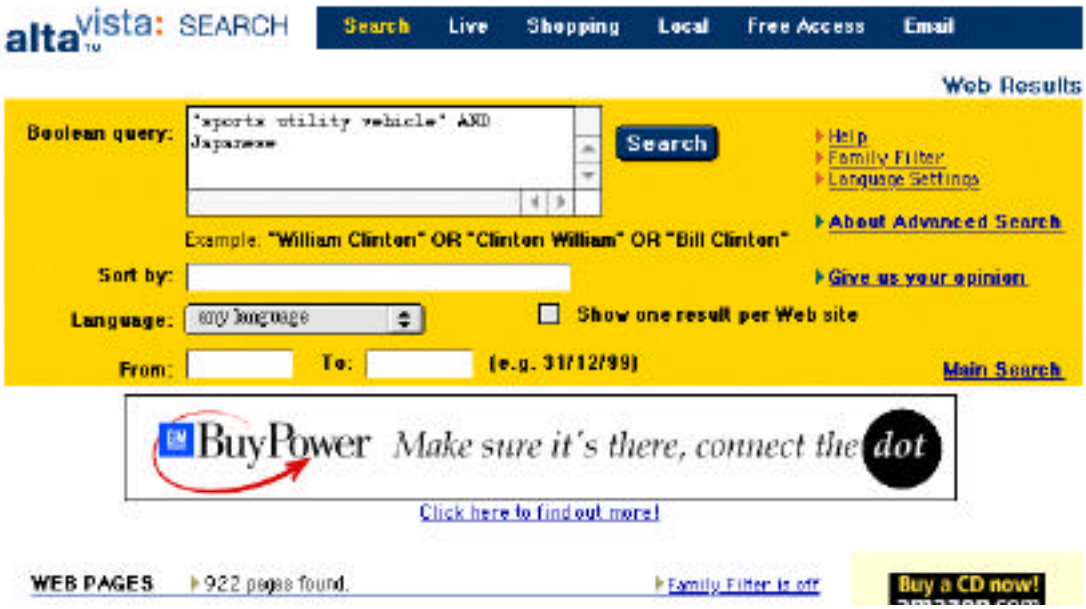
```
# Netscape HTTP Cookie File
# http://www.netscape.com/newsref/std/cookie_spec.html
# This is a generated file! Do not edit.

www.altavista.com   TRUE /         FALSE          946641602
AV_UID db87527e16ecdb
.doubleclick.net    TRUE /         FALSE
     1920499140
id   c253c4ce
.preferences.com    TRUE /         FALSE
     1258444473
PreferencesID  H9Cv05nXMh2wRdyF0vdi3q
gm.preferences.com  TRUE /         FALSE
     1258444507
CPreferencesID amm3P7ZavgaasaFfpoq8dW
```

This cookie file says that every Web site mentioned has sent a unique identifier to the Web user's computer. Every time the Web user comes back to the Web site, it, completely unbeknownst to the user, checks this cookie, modifies it and adds some

elements to it if needed. In fact, once the Web user has accepted a single cookie from this Web site, the next time he visits that site, his browser will automatically give the site access to the cookie file. (The only solution to prevent this from happening would be to systematically refuse cookies from this Web site or to delete the cookie from the cookies file after every Web surfing session.)

After accepting or refusing the cookies, here is what appears :



3. When selecting an advertisement

What happens if the Web user clicks on the General Motors ad ? He will receive a couple of cookies from the car manufacturer's server. Some of them will be sent back to the originating server. One of them will be used as a unique identifier for General Motors. Two of the cookies are shown here :

Another interesting thing to notice is the hyperlink made when clicking on the ad. It is :

http://ad.doubleclick.net/click;428940;0-8388608;1;321977;1-468|60;0|0|0;;?http://www.gmbuypower.com/cgi-bin/gx.cgi/AppLogic+COM.gm.BuyPower.applications.Session.Driver?TO=MainHomepage
It means that by activating this hyperlink, the Web user's browser is sent to DoubleClick's server. However, the page displayed will be a General Motors' Web page : http://www.gmbuypower.com/cgi-bin/gx.cgi/AppLogic+COM.gm.BuyPower.applications.Session.Driver?TO=Main.Homepage. It is in fact possible to incorporate in the HTML source code of a Web page instructions telling the browser to automatically

download another Web page or another Web site. This allows DoubleClick to know whether the Web user has showed an interest for a particular ad, so that it can sharpen its profile of this individual, can propose him other similar products, and can bill the advertisers according to a click-through billing scheme.

The link leads to this page :

4. Conclusion

An online profiling and ad-serving company like DoubleClick is able to track every Web user and leave a log of their search terms and every click on ad banner displayed on the Web sites belonging to the DoubleClick Network.
DoubleClick is able to gather such information from Web users :

- TCP/IP address ;

[11] DoubleClick has been able to give a detailed profile of the typical user of tl states that over 25 million unique individuals per month use Altavista worldwide. during work hours for business-related purposes; are predominantly male (60%); 86% of them have attended college, "the highest of any search engine"; they income of $64,000; more than half (57%) of them have conducted a purchase music CDs (19%), software (29%), travel (18%); the vast majority of them (93%) product purchase information; 90% use keywords on search engines, 81% visit company/supplier sites, 44 http://saleslogix.doubleclick.net/scripts/ slxweb.dll/leadimport?page=av.

- the Web user's prior clickstream (through the cookies) ;
- search terms typed in Altavista ;
- Ad banners already sent to the Web user ;
- Ad banners which received a positive answer (the Web user clicked on them).

As long as the same computer is used, the cookies stored on the Web user's computer enable DoubleClick to track him, even though this Web user uses several Internet Service Providers.

II. How do the information collection practices of "profiling companies" differ from those of other businesses operating on the Internet?

It is true that data is collected about individuals at Web sites and by online service providers. From the outset it is important to recognize that the activities of the online profiling companies highlights the complexity of privacy issues and the need for a broader and deeper examination of privacy on the Internet. But, the activities of these companies or the advertising networks under discussion today threaten privacy in ways that merit special consideration.

Unlike an online service provider or Web site with whom an individual initiates a relationship, advertising networks do not directly serve consumers. Rather, advertising networks establish relationships with Web sites or portals, whereby they are permitted to extract information from consumers without notifying them of the collection.

It is important to note that if a series of Web sites desired to exchange information about individuals to create the type of profiles enabled by advertising networks they would need to collect and disclose information about visitors in identifiable form. To engage in such a practice, under the Federal Trade Commission's framework a Web site would have to follow four basic Fair Information Practices when handling personal information: provide notice to consumers; gain consumer's consent prior to using data for unrelated purposes (or at least provide an opt-out); allow consumers to access and correct personal information; and provide redress to consumers where these practices are breached. Of utmost importance is the consent of the individual.

The profiling activities under discussion today fail to meet this standard in the following ways.

Notice: Fair Information Practices require individuals to be provided a description of the purpose and uses the entity makes of personal information. This notice should be clear, conspicuous, understandable and occur prior to the collection of personal information.

By and large, consumers are unaware of the profiling activities engaged in by advertising networks. Web sites do not provide individuals information about the profiling activities of advertising networks. The advertising networks themselves are unknown to consumers and if an individual learns of a companies existence it is likely to be well after data has been collected.

Individuals are not provided with notice prior to the collection of information. Nor are the notices provided by the advertising networks at their Web sites sufficient to enable consumers to make informed decisions about participation. The lack of notice is particularly troubling in this context because the collection of information by these companies is a secondary use over which individuals should have control -- in addition to effective notice.

Consent: The Fair Information Practices require businesses to gain consent prior to using personal information collected for one purpose for another purpose.

When an individual visits a Web site, enters a search term, or engages in other online activities the data generated should be used to support the activity, unless the individual has consented to additional uses. The FTC's guidance in this area requires at a minimum the right to opt-out of unrelated uses of personal information.

The profiling activities at issue here are not the purpose of the individual's interaction with the Web site. While whether the data is at this point tied to a specific known individual or tied to a unique, but not specifically identified individual is critical to the final privacy analysis, in either form it raises privacy concerns. For in this case, like the "look-up" services previously examined by the FTC, the entire business model is built upon the secondary use of the compilation of information.[12] Whether this information is used in an identifiable fashion at the start, at some other point, or never, is only one part of the equation. For the information collected and tied to a unique identifier allows businesses to make decisions about the individual and in many cases can be readily used to specifically identify the individual tracked. Faced with an attractive business model or a civil or criminal subpoena, it is extremely likely that the profiles maintained by these services in clearly identifiable form or in profiles attached to unique identifiers could identify, or at least be used to identify, individuals.

Access, Correction, and Deletion: Fair Information Practices require individuals be able to access, correct, and--if necessary--delete personal information.

The ability to see and correct information that entities maintain on you is a critical component of information privacy. Particularly when decisions are being made about the individual on the basis of such data. In this instance, individuals' experience of the Web is being altered based on information associated with their online persona. Access and correction rights must be provided here.

[12] See the FTC documents on the Individual Reference Services privacy/wkshp97/irsdoc2.htm.

Remedies: When violations of these practices occur, individuals must be able to seek relief.

It is unclear how an aggrieved individual would be made whole.

III. Heightened Risks to Individual Privacy and Consumer Trust.

The profiling activities of these companies pose unique risks to consumer privacy and consumer trust. As these companies continue to merge with themselves and offline profilers, they will hold detailed profiles on an increasingly large segment of the population. These profiles will have been created without the participation of the individual. They will have been created through the surreptitious and non-consensual collection of detailed navigational data. The profiles may become -- as the business plans and SEC disclosures of some companies portend -- fully associated with individuals, combining information about on and off line behavior.

This tracking can harm individual privacy and consumer trust in several ways.

A. Harms to Privacy

There are several individual privacy interests[13] that are at risk, and which should carry over to their interactions on the Internet, that are at risk due to these online profiling activities.

1. The Expectation of Anonymity

Imagine walking through a mall where every store, unbeknownst to you, placed a sign on your back. The signs tell every other store you visit exactly where you have been, what you looked at, and what you purchased. Something very close to this is possible on the Internet.

When individuals surf the World Wide Web, they have a general expectation of anonymity. More so than in the physical world, if an individual has not actively disclosed information about herself, she believes that no one knows who she is or what she is doing.

The introduction of networked profiling activities like those at issue here, threatens this expectation by providing a means of surreptitiously tracking and monitoring individuals' behavior. The practice of assigning unique identifiers to individuals and capturing information about every stop a person makes on the Web can lead to extremely detailed "profiles" of individuals' online lives.

2. The Expectation of Fairness and Control over Personal Information

[13] The phrase "expectations of privacy" is used here with intent. Despite case law suggesting that the legal protections afforded to our expectations of privacy are limited by the technical and social possibilities for surveillance, we believe that, as a society, we do share some basic expectations of privacy. Privacy legislation enacted by Congress in response to some of the Court's decisions lends credence to this notion.

When individuals provide information to a doctor, a merchant, or a bank, they expect that those professionals/companies will be collecting only the information needed to render the service and will use it for the sole purpose for which the information was collected. The profiling activities here depend upon surreptitious collection and the secondary use of data without necessarily having the individual's consent : the data, if they are collected for a specified purpose (a commercial transaction, sweepstakes, etc.) will be used later for other purposes (sale of consumers' profiles to third parties, use of data for data mining, etc.). In today's environment, where many entities are collecting and using personal information without adhering to the principles of Fair Information Practices, the introduction of tools and techniques of online profiling that are designed to provide a tracking device for use in e-commerce present a risk to privacy. Unlike a real world identifier, such as the Social Security Number, which an individual reveals knowingly (albeit often reluctantly) the profiling occuring online, enabled by unique identifiers, occurs without individual's knowledge and consent. While individuals may, if they are savvy, disable their cookie file, they do not have control over the collection of information about their online activities, not to mention the fact that to disable the cookie file is not the panacea to solve all the privacy problems.

The use of a single identifier across various online interactions may also enable unscrupulous individuals and those seeking to profit from information about individuals to more efficiently correlate detailed profiles. The collection of information by profiling companies at Web sites that offer products and services that reveal sensitive information about individuals such as health conditions, religious membership, and financial data raises particularly troubling privacy concerns.

B. Chilling the use of the Internet and the search for information

Surveys indicate that the fear of privacy intrusions is keeping individuals off the Internet.[14] The surreptitious tracking of individuals' behavior undertaken by the profiling companies is likely to further erode consumer confidence and trust. There is already substantial public anxiety about cookies, as this particular use of cookies becomes known, it is likely to set off additional public concern.

Tracking and monitoring of Internet usage can have a negative effect on individuals' access to information. The anonymity that the Internet affords individuals has made it an incredible resource for those seeking out information. Particularly where the information sought is on controversial topics such as sex, sexuality, or health issues such as HIV, depression, and abortion; the ability to access information without risking identification has been critical. This is not a new revelation. Protecting privacy and anonymity has consistently been recognized as an important component of ensuring full exercise of the First Amendment freedom to seek out information. But privacy is not just theoretically related to free expression. Our public policies, including laws that protect the confidentiality of library patron's records and the confidentiality of video store patron's records exist because they are critical to ensuring the public's right to read and view information.

[14] See CDT's privacy survey page: http://www.cdt.org/privacy/survey

Studies in both the online and offline world reveal that an actual or perceived lack of privacy chills individual's access to information. A 1989 study found that teenagers who used computer assisted games to gain information about pregnancy prevention sought out more information than those who were enrolled in health education classes.[15] As one of the reasons for pursuing computer assisted health education, the authors stated that "Patients have indicated that they prefer computer to human interviewing or advice regarding sensitive topics such as sexuality. Computer-assisted instruction has been shown to enhance interactive skills with regard to sexuality without the sensitive personal exposure of class or group sessions."[16] The privacy and confidentiality provided by computer-assisted education was critical to ensuring that students sought out desired information. Similarly, a more recent study found that online access was critical to gay youths' ability to come to terms with their sexual orientation. The ability to gain information without risking exposure of their identity was pivotal.[17]

IV. Conclusion

The profiling activities of these advertising networks pose a significant risk to consumers' privacy. Individuals should not be the subject of this profiling -- whether it is occurring in fully identifiable form or through the use of a unique identifier -- against their will. At this time, we believe that individual's informed consent must be obtained by these companies prior to the collection of personal information from consumers. This issue merits additional consideration by the Commission.

The surreptitious creation of detailed dossiers of individuals' online behavior has the potential to transform the World Wide Web from a largely anonymous environment into one where individuals are continuously monitored and in some cases fully identified. If the practices of these companies are allowed to spread unchecked we believe that individuals' control over the use and disclosure of their personal information will be further eroded. Survey after survey informs us that the surreptitious collection and compilation of data represented by these companies breeds consumer mistrust.

The proliferation of these profiling systems will needlessly erode anonymity and expand the practice of collecting personal information from Web site visitors without proper notice to them and without their consent. The segment of the online business community that has committed itself to promoting more responsible practices in the online environment may find its work to increase consumer participation and trust undermined. Studies have found that the collection of information and the tracking of individuals' activities makes individuals' reluctant to participate in online life.

Technical and policy solutions must be developed that provide strong protections for individual privacy and anonymity, and allow individuals to benefit from the

---

[15] Adolescent Pregnancy Prevention by Health Education Computer Ga
Instruction of Knowledge and Attitudes, David M. Paperny et. al, Pediatrics Vol. 83 No. 5, May 1989.

[16] Id.

[17] 1997 survey conducted by Oasis Magazine and !OutProud!, the National
Bisexual and Transgender Youth, reported that 68% of gay youth were able to
sexual orientation as a result of online access. (See letter submitted by GLAA
1999.

customization possible on the Web. The practices of the advertising networks do not meet this standard.

Appendix :

Terms, Definitions and Description

Concept of HTTP
Stands for "HyperText Transport Protocol". It is the protocol used between a Web browser and a Web server. The Web browser sends an HTTP request to a Web server (a Web site) and gets an HTTP answer including the Web page in HTML code.

Distinction between explicit and implicit hyperlinks[18]
An explicit hyperlink is a hyperlink that appears on a Web page (they are generally underlined and in blue) and which refers the Web user to another Web page when he clicks on it.
An implicit (or invisible) hyperlink automatically links the Web user's browser to an HTML document, either located on the same server or on another one (it is also called inlining). The browser does not need the Web user's intervention to download this HTML document. The Web user may sometimes notice that such a hyperlink is executed on his browser by paying attention to the display of packets of information downloaded when accessing a web page and displayed at the bottom of the browser. When the browser reads that an HTML document contains an HTTP request, it opens a new HTTP session with the web site indicated by the HTTP request, while downloading the current web page. This is what is happening when a Web site displays ad banners : the Web page contains an HTTP request to another Web site that will send an image file containing the banner.

[18] Cfr Jean-Marc DINANT, Les traitements invisibles sur Internet, http://www.droit.fundp.ac.be/crid/eclip/luxembourg.html.