

Simson L. Garfinkel

September 28, 2000

Prepared Statement of

Simson L. Garfinkel

Before the

**Senate Committee on Commerce, Science, And
Transportation**

On

S.809: "Online Privacy Protection Act of 1999"

S.2606: "Consumer Privacy Protection Act"

S.2928: "Consumer Internet Privacy Enhancement Act"

Mr. Chairman and members of the Committee, I am honored to speak before you today.

My name is Simson Garfinkel. I am perhaps best known in the field of consumer privacy because of my book *Database Nation: The Death of Privacy in the 21st Century*, which was published this January. As a journalist, I have written about intersection of privacy and information technology for more than twelve years. Besides *Database Nation*, I am the co-author of five books on computer security. Finally, I am an experienced technologist and an entrepreneur. I have had an Internet e-mail address since 1983. In 1995, I started Vineyard.NET, an Internet Service Provider on Martha's Vineyard. In 1998, I started a company called Sandstorm Enterprises, which develops advanced computer security tools. I am currently the Chief Scientist at Broadband2Wireless, a company that is building a nation-wide high-speed wireless Internet service. I also serve as an advisor to two firms that sell privacy-related products and services. I must say, however, that I am here speaking for myself, for none of the companies with which I am currently affiliated.

Mr. Chairman, as you know, many surveys have found that Americans are very concerned about the growing number of threats to their privacy. Other surveys have found that many Americans are refusing to participate in e-commerce on the Internet, because they are fearful that they will be compromising their privacy in the process. Indeed, I have many friends who do not use the Internet to make purchases, to view their bank statements, or to pay their bills. Some of these friends are extremely sophisticated individuals: they feel that by making use of e-commerce, they will be putting their personal information at risk, and that they might become victims of fraud as a result. It's hard to argue with this point of view given the dramatic rise in identity theft that we have seen in recent years.

In any event, this January, after my book was published, I went on a book tour around the country. I spoke with many Americans about privacy, both on and off the Internet. Most of the people that I spoke with realized that there were few if any protections for their personal information in Cyberspace. What you might find more revealing, however, is that few Americans realized how poorly their privacy is protected off the Internet. Although Congress has passed a whole slew of privacy laws over the past twenty years, it really is a legislative patchwork. There are many basic protections that Americans feel they do have, but which in fact they do not. For example, many Americans do not realize that stores routinely engage in covert video surveillance, and that there is no legal requirement to notify shoppers that such surveillance is taking place.

One of the points that I make when I speak about privacy is that Americans tend to approach electronic privacy issues as a big *tabula rasa*, an uncharted ocean, if you will, in which there are many questions and few answers. Yet for more than 25 years we've had a consistent set of principles that do a wonderful job confronting and solving these electronic privacy issues. I am speaking, of course, of the Code of Fair Information Practices, as well as the refinements on the code that have been made over the years.

The reason that the principles in the CFIP have been around so long is that they resonate with our basic democratic beliefs. The CFIP was developed for the information age, and I think that these practices can and should be extended to the Internet.

All of the bills that you are considering embody aspects of the CFIP. I believe that S.2606 goes further and does a better job protecting the interests of Americans. In the rest of my time, I'd like to explain why.

Each and every bill you are considering require businesses to state their policies regarding the collection of personal information. But what then? After **notice**, I believe that **access** is a value that is central to our principles of fair play and justice.

Access

Imagine that you learned of a company that was in the business of collecting and selling large amounts of personal information. You contact the company and ask them if they

have a file on you. They say that they won't tell you. You ask if you can see the contents of your file. The company says "no." You ask if you can have a list of the other firms to which your personal information has been transferred. The company responds that it is impossible to create such a list, and even if it were, that information is trade secret.

You can imagine how frustrated and how powerless you would feel.

This is the situation that confronted most Americans in the 1960s. The companies were credit reporting agencies like Retail Credit (now Equifax) and TRW (now Experian.) When Congress considered legislation that ultimately became the Fair Credit Reporting Act, those companies insisted that giving consumers access to their credit reports would be unworkable, a tremendous economic burden, and would be subject to abuse. Today, nearly 30 years later, we view access to credit reports as a fundamental right.

As a technologist, I can tell you that it is granting an individual access to their personal information is much easier to do today than it was 30 years ago. Consider the case of cookies and Doubleclick. I have met many people who do not want an internet advertising firm such as Doubleclick watching over their shoulder and keeping track of every website they visit, every article that they read. They see that Doubleclick has put a cookie on their computer and they want to know what Doubleclick's computer's have in the databanks.

Now Doubleclick's computer's consult this database every single time they show a banner advertisement over the Internet. Doubleclick prides itself on this capability --- it is Doubleclick's value added. The company even has a patent on the technology, US5,948,061: a "Method of delivery, targeting, and measuring advertising over networks." It would be a simple matter to turn this technology around so that when a user visits the Doubleclick site, the Doubleclick computers would report the personal information that they have on file about the individual.

Consent

Beyond the issue of access, the issue of Consent is paramount to any discussion of online privacy.

An overwhelming number of Americans that I have spoken with believe that they own their personal information. It's true that this information runs contrary to US law. Nevertheless, it is a deeply held belief among the vast majority of Americans.

The bills that you have for consideration before you take two very difficult views of personal information ownership. By creating a so-called "opt-out" regime, S.809 and S.2928 essentially give ownership of personal information to corporations and businesses. These bills tell Corporate America: "you can do anything you want with a consumer's personal information, unless that consumer has the knowledge and the foresight to tell you otherwise."

I submit to you that this approach is inherently unfair.

Many Americans complain about telemarketing calls that they receive during dinnertime. When I was writing the book *Database Nation*, I was surprised to learn that Americans have been complaining about these nightly interruptions for more than **thirty-five years**. Now for many years the Direct Marketing Association has operated its so-called Telephone Preference Service that lets Americans put their phone numbers on a "do-not call list." But few Americans know that these services even exist.

Now many people think that privacy policies and the use of personal information are solely issues having to do with junk mail, telemarketing calls, and spam e-mail. This is not the case. As we move into the 21st Century, there is a vast array of actions that Internet-savvy firms will be able to perform with our personal information. It will be difficult for us to keep track of all the ways that our personal information can and will be exploited. It will be nearly impossible for us to meaningfully opt-out.

Consider this hypothetical example. What if a company were to electronically rifle my online address book, get the list of every person that I correspond with, and then send each one an e-mail message? What if these e-mail messages claimed to be from me, and contained endorsements of the company's new product? What if the company had an opt-out privacy policy, but it was so complicated to opt-out that few people understood what was being done with their personal information until it was too late? This Committee might very well hold hearings to investigate the company, alleging that the practices were illegally appropriating the personal information and identities of consumers. As it turns out, technologies that appropriate e-mail address books are already being deployed. I have attached to the end of my written testimony an article written by Boston Globe columnist Hiawatha Bray which alleges that Microsoft is using a technique such as this to market its new MSN server. Indeed, the only reason that Mr. Bray did not inadvertently send out thousands of e-mail to every person in his address book when he tried out Microsoft's new MSN server is that the service first asked Mr. Bray's permission --- that is, the service abides by an opt-in policy.

An opt-in regime is inherently more democratic than an opt-out one. With opt-in, companies explain to consumers what will be done with their personal information, and then it's up to the consumer to decide whether or not they wish to participate. This is the same sort of "informed consent" system that has become the standard in medicine, banking, and other areas.

One of the growing critiques of the opt-out approach favored by S.809 and S.2928 is that these policies require consumers to read, understand, and act upon the so-called "privacy policies" posted by websites. Unfortunately, these policies are frequently difficult-to-understand and do little to protect privacy. To demonstrate how opaque these privacy policies are, I've attached the "DoubleClick Privacy Statement" at the end of my written testimony. I have a master's degree in journalism, I've written a book on privacy, and I've

taken courses at law school, and I really don't understand what DoubleClick is with personal information. The advantage of an opt-in regime is that, in an opt-in regime, if a company does clearly explain its practices and their advantages to consumers, the resultantly confused consumers will have reason to opt-in.

As I said before, most Americans believe that they own their personal information. But ownership really isn't the right word. As I make clear in my book *Database Nation*, what is owned can be transferred or sold. American's view of their own privacy is much closer to the French notion of moral rights. Americans feel that they have a right to privacy protection. They feel that they have a right to have companies protect their privacy unless they give explicit permission otherwise. Americans feel they have a right to be let alone. Americans want to live in an opt-in system. Opt-out is contrary to our democratic principles and heritage.

Enforcement

Once concern that I have with all of the bills that you are currently considering is the issue of enforcement. I think that it makes sense to have a single agency within the US government that is responsible for enforcing privacy laws. Right now, that agency seems to be the Federal Trade Commission. I'm not sure that the FTC is the right choice --- I would like to see an independent Privacy Office that's responsible for both the commercial sector and for the laws that apply to the Federal Government and to the laws that are enforced through the FCC. I think that it makes sense to build a center of expertise within the federal government. I think that a Privacy Office could be a resource to the rest of the Federal Government, and to private industry as well.

But I understand that this Congress is unlikely to create a Privacy Office and that the Federal Trade Commission seems to be the current privacy torchbearer. Indeed, the Commission did an excellent job on its recent privacy study. I'm pleased that S.2606 would create a FTC Office of Online Privacy.

I am however concerned that both S.2928 and S.2606 split enforcement between the Federal Trade Commission and an assortment of other federal agencies. I understand that there are technical reasons for doing this, but I think that they should be reconsidered.

I am very pleased that S.2928 establishes a statutory civil penalty of \$22,000 for each privacy violation. Traditionally, one of the hardest problems for those faced with privacy violations has been to demonstrate damages. Likewise, creation of a private right of action in S.2606, with awards up to \$50,000 for willful and knowing violations, will make it far easier for wronged individuals to pursue compensation in our courts. This may be an effective deterrent.

I think that S.2606's protection of Whistleblowers (section 305) is an important protection that is missing from the other bills under consideration. Often times the privacy abuses

that occur within an organization are unknown to outsiders. In these cases, it is important to encourage insiders to step forward, and the protection for whistleblowers will create protections for these individuals.

In this age of mega-corporations, a vast amount of personal information could be collected and used in a manner that could be considered "solely for internal company processes." For this reason, I think that the exemption for "internal company processes" in S.809 is a dangerous precedent. Company policies should not be exempt from privacy legislation simply because they do not involve third-parties.

Bankruptcy is a real threat faced by many organizations that collect personally identifiable information. It is very important that information collected by an organization when it is financially healthy not be auctioned off to the highest bidder during a bankruptcy proceeding. S.2606 takes personally identifiable information off the table of the bankruptcy courts. This is a very important provision that should be echoed by the other legislation under consideration.

I am also concerned that the legislation under consideration does not adequately address non-commercial threats to privacy. For example, exempting non-profit organizations, such as S.2928 does, would allow public radio stations to engage in privacy abuses in the interest of fund raising. As we know, this has happened in the past; I would like to see legislation prohibit such abuses from happening on the Internet in the future.

In Conclusion

Mr. Chairman, I believe that the United States will eventually have some form of legislation that protects consumers' personal information, both on and off the Internet. I believe that such legislation is vital to the long term health of democracy in this country.

What I do not know, Mr. Chairman, is whether comprehensive privacy-protecting legislation will be passed this year, next year, or in twenty years. I do know that the longer the US Congress waits to pass such legislation, the more economic dislocation there will be when it is final passed. That is because the longer you wait, the more businesses will spring up whose business model depends upon misrepresentation and privacy invasion. There are a few such companies now; with no action, there will be more next year.

Nevertheless, I think that it would be foolish to delay the passage of legislation that protects online privacy while the Congress tries to create that comprehensive privacy legislation.

The American people believe that they have a right to privacy, and they wish to see this body pass legislation that affirms that right. Paramount to protecting the right to privacy in the digital age is the rights of individuals to have access to their own information, and the right to have their information protected and held in trust unless they explicitly give

permission for it to be used otherwise. I therefore cannot support S.809 and S.2928, because both of these bills would create an opt-out regime. Instead, I would urge this body to make S.2606 the basis of any privacy legislation that is approved by this committee.



THIS STORY HAS BEEN FORMATTED FOR EASY PRINTING

UPGRADE

Microsoft serves up its own spam

By Hiawatha Bray, Globe Columnist, Globe Staff, 9/28/2000

Sometimes I feel like that ape in the beginning of the movie "2001." There he is, starving amidst a pile of animal bones. He's so stupid that it takes a singing black slab from outer space to make him grab a tibia and go kill something. Couldn't he just figure it out on his own?

I felt that way yesterday as I read of the latest outrage involving unwanted e-mail, better known as spam. I am, of course, opposed to it. And so, ostensibly, is Microsoft Corp, which has built antispam features into its e-mail software and its Web-based Hotmail service.

This makes me wonder why Microsoft is presently engaged in a massive spam campaign of its own, one that features the unwitting participation of many Internet users. But I'm even more puzzled by the fact that evidence of the outrage landed in my lap, and I ignored it.

A few weeks back, I installed the preview version of the new Explorer software for Microsoft's MSN online service. Basically, Microsoft has customized its Internet Explorer browser with specialized links that mimic the features found on America Online. It's a pretty good job. MSN Explorer's extra clutter isn't to my taste, but newbies may find it congenial.

Anyway, after installing the MSN software, I was invited to click a check box that would have sent e-mails to my friends to announce the joyous event. This should have got me thinking.

Instead, I did what I almost always do when installing Internet software. I clicked "no thanks" and forgot all about it.

Alas, not every user of the new software was so cautious. That's why I received an e-mail last week from a reader who was hopping mad about getting an unsolicited advertisement from Microsoft, sent to him by some guy he'd never heard of.

The reader fired off a complaint to Microsoft, and got this reply: "When a user installs MSN Explorer, they have the option of sending an e-mail from MSN Explorer to invite you to use the program. This is not an advertisement or commercial e-mail sent to solicit information from you by MSN - it is only an invitation sent by an individual member to try the new product."

This didn't satisfy the reader, but incredibly, it satisfied me. Here's my response: "Well, that's not quite spam, is it? Maybe it's a questionable tactic, but it was sent by someone you presumably know."

Proof positive that too much e-mail makes you stupid. Had I not been so swamped with the stuff, I might have put two and two together.

After all, I'd written quite a bit on the Melissa computer virus - the one that automatically sent copies of itself to every e-mail address on a victim's computer. Melissa, you'll recall, only affected users of Microsoft's e-mail software.

So I had all of the pieces of the puzzle, and only needed to snap them together. I didn't. But others did, and by yesterday morning it was the talk of the Web.

Sure enough, the MSN software, unless you tell it otherwise, will check to see if your computer has a copy of Microsoft's Outlook Express e-mail program. If it's there, the software then checks the program's address book, scoops up all of the e-mail addresses contained therein, and sends them an "invitation" to join MSN. This invitation is, of course, signed by you.

If I hadn't clicked the "don't you dare" box while installing MSN Explorer, I'd have sent this warm, personal invitation to 2,290 of my nearest and dearest friends. That's how many names are in my Outlook Express address book. These are mostly tech-industry types who'd have held me in even lower regard than they already do once this personalized spam arrived. For spam is exactly what this is, and of a particularly insidious kind.

Granted, MSN Explorer asks for permission before cranking out the mail. But how many users realize that they'll be sending advertisements for Microsoft? How many understand that they're sending these ads to their bosses, their bookies, their best customers - everybody?

I understand that Microsoft is frustrated; MSN has 3 million users to AOL's 24 million. But I never thought they'd stoop to the favorite market tool of Internet pornographers. Somebody at MSN had a brainstorm, but then failed to think it through. I guess we need a couple more of those black slabs. Put one in the MSN marketing department, and the other next to my desk.

Hiawatha Bray is a member of the Globe Staff. He can be reached by e-mail at

Testimony of Simson L. Garfinkel, October 3, 2000
Page 10

bray@globe.com.

This story ran on page E01 of the Boston Globe on 9/28/2000.
© [Copyright](#) 2000 Globe Newspaper Company.

September 28, 2000

DoubleClick Privacy Statement

Internet user privacy is of paramount importance to DoubleClick, our advertisers and our Web publishers. The success of our business depends upon our ability to maintain the trust of our users. Below is information regarding DoubleClick's commitment to protect the privacy of users and to ensure the integrity of the Internet.

Information Collected in Ad Delivery

In the course of delivering an ad to you, DoubleClick does not collect any personally-identifiable information about you, such as your name, address, phone number or email address. DoubleClick does, however, collect non-personally identifiable information about you, such as the server your computer is logged onto, your browser type (for example, Netscape or Internet Explorer), and whether you responded to the ad delivered.

The non-personally identifiable information collected by DoubleClick is used for the purpose of targeting ads and measuring ad effectiveness on behalf of DoubleClick's advertisers and Web publishers who specifically request it. For additional information on the information that is collected by DoubleClick in the process of delivering an ad to you, please .

However, as described in "Abacus Alliance" and "Information Collected by DoubleClick's Web Sites" below, non-personally identifiable information collected by DoubleClick in the course of ad delivery *can be associated with a user's personally identifiable information* if that user has agreed to receive personally-tailored ads.

In addition, in connection solely with the delivery of ads via DoubleClick's DART technology to one particular Web publisher's Web site, DoubleClick combines the non-personally-identifiable data collected by DoubleClick from a user's computer with the log-in name and demographic data about users collected by the Web publisher and furnished to DoubleClick for the purpose of ad targeting on the Web publisher's Web site. DoubleClick has requested that this information be disclosed on the Web site's privacy statement.

In addition, in connection solely with the delivery of ads via DoubleClick's DART technology to one particular Web publisher's Web site, DoubleClick combines the non-personally-identifiable data collected by DoubleClick from a user's computer with the log-in name and demographic data about users collected by the Web publisher and furnished to DoubleClick for the purpose of ad targeting on the Web publisher's Web site. DoubleClick has requested that this information be disclosed on the Web site's privacy statement.

There are also other cases when a user voluntarily provides personal information

in response to an ad (a survey or purchase form, for example). In these situations, DoubleClick (or a third party engaged by DoubleClick) collects the information on behalf of the advertiser and/or Web site. This information is used by the advertiser and/or Web site so that you can receive the goods, services or information that you requested. Where indicated, DoubleClick may use this information in aggregate form to get a better general understanding of the type of individuals viewing ads or visiting the Web sites. Unless specifically disclosed, the personally-identifiable information collected by DoubleClick in these cases is not used to deliver personally-tailored ads to a user and is not linked by DoubleClick to any other information.

Abacus Alliance

On November 23, 1999, DoubleClick Inc. completed its merger with Abacus Direct Corporation. Abacus, now a division of DoubleClick, will continue to operate Abacus Direct, the direct mail element of the Abacus Alliance. In addition, Abacus has begun building Abacus Online, the Internet element of the Abacus Alliance.

The Abacus Online portion of the Abacus Alliance will enable U.S. consumers on the Internet to receive advertising messages tailored to their individual interests. As with all DoubleClick products and services, Abacus Online is fully committed to offering online consumers **notice** about the collection and use of personal information about them, and the **choice** not to participate. Abacus Online will maintain a database consisting of personally-identifiable information about those Internet users who have received notice that their personal information will be used for online marketing purposes and associated with information about them available from other sources, and who have been offered the choice not to receive these tailored messages. The notice and opportunity to choose will appear on those Web sites that contribute user information to the Abacus Alliance, usually when the user is given the opportunity to provide personally identifiable information (e.g., on a user registration page, or on an order form).

Abacus, on behalf of Internet retailers and advertisers, will use statistical modeling techniques to identify those online consumers in the Abacus Online database who would most likely be interested in a particular product or service. All advertising messages delivered to online consumers identified by Abacus Online will be delivered by DoubleClick's patented DART technology.

Strict efforts will be made to ensure that all information in the Abacus Online database is collected in a manner that gives users clear notice and choice. *Personally-identifiable information in the Abacus Online database will not be sold or disclosed to any merchant, advertiser or Web publisher.*

Name and address information volunteered by a user on an Abacus Alliance Web site is associated by Abacus through the use of a match code and the DoubleClick cookie with other information about that individual. Information in the Abacus Online database includes the user's name, address, retail, catalog and online

purchase history, and demographic data. The database also includes the user's non-personally-identifiable information collected by Web sites and other businesses with which DoubleClick does business. Unless specifically disclosed to the contrary in a Web site's privacy policy, most non-personally-identifiable information collected by DoubleClick from Web sites on the DoubleClick Network is included in the Abacus Online database. However, the Abacus Online database will not associate any personally-identifiable medical, financial, or sexual preference information with an individual. Neither will it associate information from children.

Sweepstakes

DoubleClick's Flashbase, Inc. subsidiary provides automation tools that allow our clients to provide online contests and sweepstakes ("DoubleClick sweepstakes").

All DoubleClick sweepstakes entry forms must provide a way for you to opt-out of any communication from the sweepstakes manager that is not related to awarding prizes for the sweepstakes. Entry forms must further provide consumers with a choice whether to receive email marketing materials from third parties. When you enter a DoubleClick sweepstakes, the information you provide is not be shared with DoubleClick or any third party, unless you agree by checking the opt-in box on the sweepstakes entry form. If you enter a sweepstakes, you agree that the sweepstakes sponsor may use your name in relation to announcing and promoting the winners of the sweepstakes. See the official rules of the sweepstakes you are entering for additional information.

DoubleClick does collect aggregate, anonymous information about the sweepstakes. That information is primarily used to help sweepstakes managers choose prizes and make other decisions regarding the organization of the sweepstakes. DoubleClick does not associate information provided through the sweepstakes with your other web browsing activities or clickstream data.

Email

DoubleClick uses DARTmail, a version of DART technology, to bring you emails that may include ads. Email is sent only to people who have consented to receive a particular email publication or mailing from a company. If at any time you would like to end your subscription to an email publication or mailing, follow either the directions posted at the end of the email publication or mailing, or the directions at the email newsletter company's Web site.

In order to bring you more relevant advertising, your email address may be joined with the information you provided at our client's website and may be augmented with other data sources. However, DoubleClick does not link your email address to your other Web browsing activities or clickstream data.

Information Collected by DoubleClick's Web Sites

The Web sites owned or controlled by DoubleClick, such as www.NetDeals.com

and www.IAF.net may ask for and collect personally-identifiable information. DoubleClick is committed to providing meaningful notice and choice to users before any personally-identifiable information is submitted to us. Specifically, users will be informed about how DoubleClick may use such information, including whether it will be shared with marketing partners or combined with other information available to us. In most cases, the information provided by a user will be contributed to the Abacus Online database to enable personally-tailored ad delivery online. Users will always be offered the choice not to provide personally-identifiable information or to have it shared with others.

Access

DoubleClick offers users who have voluntarily provided personally-identifiable information to DoubleClick the opportunity to review the information provided and to correct any errors.

Cookies and Opt Out

DoubleClick, along with thousands of other Web sites, uses cookies to enhance your Web viewing experience. DoubleClick's cookies do not damage your system or files in any way.

Here's how it works. When you are first served an ad by DoubleClick, DoubleClick assigns you a unique number and records that number in the cookie file of your computer. Then, when you visit a Web site on which DoubleClick serves ads, DoubleClick reads this number to help target ads to you. The cookie can help ensure that you do not see the same ad over and over again. Cookies can also help advertisers measure how you utilize an advertiser's site. This information helps our advertisers cater their ads to your needs.

If you have chosen on any of the Web sites with which Abacus does business to receive ads tailored to you personally as part of Abacus Online's services, the cookie will allow DoubleClick and Abacus Online to recognize you online in order to deliver you a relevant message.

However, if you have not chosen to receive personally-targeted ads, then the DoubleClick cookie will *not* be associated with any personal information about you, and DoubleClick (including Abacus) will not be able to identify you personally online.

While we believe that cookies enhance your Web experience by limiting the repetitiveness of advertising and increasing the level of relevant content on the Web, they are not essential for us to continue our leadership position in Web advertising.

While some third parties offer programs to manually delete your cookies, DoubleClick goes one step further by offering you a "blank" or "opt-out cookie" to prevent any data from being associated with your browser or you individually. If

you do not want the benefits of cookies, there is a simple procedure that allows you to deny or accept this feature. By denying DoubleClick's cookies, ads delivered to you by DoubleClick can only be targeted based on the non-personally-identifiable information that is available from the Internet environment, including information about your browser type and Internet service provider. By denying the DoubleClick cookie, we are unable to recognize your browser from one visit to the next, and you may therefore notice that you receive the same ad multiple times.

If you have previously chosen to receive personally-tailored ads by being included in the Abacus Online database, you can later elect to stop receiving personally-tailored ads by denying DoubleClick cookies.

Your opt-out will be effective for the entire life of your browser or until you delete the cookie file on your hard drive. In each of these instances, you will appear as a new user to DoubleClick. Unless you deny the DoubleClick cookie again, DoubleClick's ad server will deliver a new cookie to your browser.

If you would like more information on how to opt-out, please .

Disclosure

DoubleClick makes available all of our information practices at www.doubleclick.net, including in-depth descriptions of our targeting capabilities, our privacy policy, and full disclosure on the use of cookies. In addition, we provide all users with the option to contact us at with any further questions or concerns.

Security

DoubleClick will maintain the confidentiality of the information that it collects during the process of delivering an ad. DoubleClick maintains internal practices that help to protect the security and confidentiality of this information by limiting employee access to and use of this information.

Industry Efforts to Protect Consumer Privacy

DoubleClick is committed to protecting consumer privacy online. We are active members of the Network Advertising Initiative, NetCoalition.com, Online Privacy Alliance, Internet Advertising Bureau, New York New Media Association, and the American Advertising Federation.

For more information about protecting your privacy online, we recommend that you visit www.nai.org, www.netcoalition.com, and www.privacyalliance.org. If you have any additional questions, please contact us at .

We also recommend that you review this Privacy Statement periodically, as DoubleClick may update it from time to time.

1973: The Code of Fair Information Practices

The Code of Fair Information Practices was the central contribution of the HEW (Health, Education, Welfare) Advisory Committee on Automated Data Systems. The Advisory Committee was established in 1972, and the report released in July. The citation for the report is as follows:

U.S. Dep't. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens (1973).

The Code of Fair Information Practices is based on five principles:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

1980: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

Today privacy advocates have moved beyond the 1973 Code of Fair Information Practices and have adopted the OECD's 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. You can find the [entire document on the OECD website](#). The most important principles are:

Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

- a. with the consent of the data subject; or
- b. by the authority of law.

Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

An individual should have the right:

- a. To obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
- b. To have communicated to him, data relating to him
 - o *within a reasonable time;*
 - o *at a charge, if any, that is not excessive;*
 - o *in a reasonable manner; and*
 - o *in a form that is readily intelligible to him;*
- c. To be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
- d. To challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

A data controller should be accountable for complying with measures which give effect to the principles stated above.