Web Bugs: An invasion of Privacy or Better Business Assistant?
Rich Gresham
GSEC Practical version 1.2f
December 18, 2001

In George Orwell's book **Nineteen Eighty-four** Winston Smith works for the Ministry of Truth, rewriting and altering records of the past, Winston begins to question the ruling party and wondering if their direction was the best for the individual and mankind. In every room of each person's homes, there are telescreens to force the political propaganda of the New World Order. These telescreens also contain a camera and a microphone so that "Big Brother" is always watching you.

In today's world of the Internet do we face our own "Brave New World?" Just as Winston grows to fear "Big Brother" watching over him, some Internet browsers and all privacy advocates fear some the new tools that have come to the web in the last few years. We all know about cookies and have come to expect them in conjunction with our ability to walk the web. Banner ads and cookies seem to come together on almost every popular web site and on many search engine starting points. The modern browsers allow you to turn off cookies or to prompt you when a site wants to leave a cookie on your PC. There are programs available so that you can use anonymous cookies instead of baring all to the world, but did you know that the little one-pixel gif called a web bug slips right by all of these settings?

Let's begin our own tour of our "Brave New World" of Internet business by examining the web bug. First we will find out what one is and how it works. Then we will examine how it is used and how it could be misused to invade our privacy. We will conclude with some privacy policy points that we, as security advisors to the business world, need to make to help protect ourselves and our consumers and finally some methods of fighting against web bugs.

What are these "web bugs" and why are they called bugs? They are small graphics tags embedded in a web page or e-mail, usually invisible to the browsing consumer. They are used to track a location in cyberspace. Some businesses use web bugs to track "hits" on a web page so that they can better serve the consumer. Because of what these one-pixel gifs can be used for, the privacy advocates call them eavesdropping devices, or "bugs." There are usually three computers involved in one of these web bug transactions. The originator is our innocent consumer searching the web for some new gadget for the computer who goes to www.newgadgets.com, the intended web site. This home web page has a web bug embedded in it. When the originator's browser starts to load the web page, it comes to the embedded web bug that says that the image is actually at techbaseinfo.com, the hidden web The originator (or party of the first part) is our innocent consumer searching the web for some new gadget for the computer who goes to www.newgadgets.com, the intended web site. This home web page has a web bug embedded in it. When the originator's browser starts to load the web page, it comes to the embedded web bug that says that the image is actually at techbaseinfo.com, the hidden web site. Usually, web bugs are represented as HTML IMG tags.

For example, here are two Web bugs recently found on Quicken's home page (www.quicken.com):

> <img src="http://ad.doubleclick. net/ad/pixel.quicken/NEW" width=1 height=1 border=0><IMG WIDTH=1 HEIGHT=1border=0SRC= "http://media.preferences.com/ping? ML_SD=IntuitTE_Intuit_1x1 _RunOfSite_Any&db_afcr=4B31-C2FB-10E2C&event= reghome&group=register&time= 1999.10.27.20.5 6.37">
> The two Web bugs were placed on the home page by Quicken to provide "hit" information about visitors to DoubleClick and MatchLogic (AKA, preferences.com), two Internet advertising companies. [1]

In e-mail, web bugs act similarly. The originator opens their e-mail, when the program gets to the embedded graphic; an attempt is made to go to the hidden web site where information is left without the e-mail recipient ever knowing about it.

Should we be concerned about whether or not a web site uses these hidden tags when all they are doing is acting as "hit" counters? Well, as you may have suspected, a web bug can do more than just register a "hit." There is a host of additional information that a web bug can pass to the hidden web site:

The browser's IP address
The web bug's originating URL page
The URL of the web bug image, which contains the information to be communicated between the web page and the collecting server
The time the bug was viewed
The type of web browser used
A previously set cookie value [2]

Web bugs can even exchange information with existing cookies on a computer if they are both from the same web site or advertising company, such as DoubleClick, which uses web bugs and dominates the advertising market. While most people are aware that web sites use cookies, especially when they see banner ads, few know about web bugs because they are not seen and anti-cookie filters or programs do not catch web bugs.

Other businesses use different tools to gather measurements, for example placing web bugs on web pages, according to Cyveillance, an Internet strategic business analysis and trend company based in Virginia. Cyveillance says the use of web bugs has increased 488 percent in the past three years. This is based upon their random sampling of over one million web pages. "Eight out of the top fifty brands web sites contain web bugs in their home pages." [3]

Businesses use web bugs as tools for measurement. The kinds of things that they are used for are:

Count web page hits
Track web site use, page by linked page
Track web page linking across web sites
Count the number of times a banner ad has appeared

- Measure the effectiveness of a banner ad by matching visits to a site with banner ads
- Match a purchase with a banner ad
- Allow a third party server to provide logging services for a web site that cannot do so
- Record and report web browser type and configuration for content viewing
- Transfer previously input demographic data from a web site to an Internet marketing company
- Transfer previously input personal information from a web site to an Internet marketing company
- To synchronize cookies between two companies. This data can be demographic or personal

For e-mail mass mailings, web bugs are used for similar reasons:

- If a particular e-mail message was read
- When the message was read
- If the message was forwarded to others

Businesses say that the information gathered is used to provide a better surfing experience for the consumer. Presentations for the consumer are customized based upon past purchasing and current browsing experiences. This information, according to the business community, is held in strictest confidence. In e-mail marketing campaigns, web bugs:

- Are used to count how many who read the message so that they can tell how effective the marketing campaign was
- Are used to identify who did not read the message so that they can be removed from future e-mail campaigns
- Can be used to synchronize a cookie to their particular e-mail address so that if the consumer visits the web site later, the marketer will know.

All of this sounds like the perfect fit for businesses and consumers. There is another side to the tale of web bugs that is presented by privacy advocate groups. While the web bug itself is not the culprit, the fact that you visited a particular web site is registered somewhere in the world before that web site is loaded into your browser. With the exchange of information between the web bug and existing cookies, personal information such as your name, address and phone number can be tied to a visit to a particular web site. Let's imagine what could happen: your doctor is researching some new medication for stomach ulcers at a pharmaceutical web site that has web bugs on various pages. Even before the information the doctor is searching for has been downloaded to his computer, the hidden server that the web bug reports to finds out that the doctor is looking for information on stomach ulcers. The doctor's e-mail, name and phone number are transferred to the hidden web site for contact by the sales department later. All of this happens without the doctor knowing it. Imagine that the hidden web site was operated by unscrupulous people. The knowledge they could gain without anyone's knowledge is frightful since medical records as well as patient-doctor relationships are legally protected.

Unbelievable, or too far-fetched you say? Can we be living in the "Brave New World" of George Orwell where the political system of Doublethink takes the old records and throws them into the Memory Hole where they are burnt and replaces them with altered records? In November of 1999, DoubleClick bought Abacus Direct, a company that markets consumer-purchasing data to catalog firms, to gain detailed personal profiles on more than ninety percent of U. S. Households and planned on linking the data bases of the two companies. This is not to suggest that DoubleClick or Abacus Direct would ever alter records as Orwell has Doublethink doing in his book.

In the CNET news.com article dated March 1, 2000, the consumer advocacy group, Center for Democracy and Technology, filed a report with the Federal Trade Commission alleging "potential privacy violations in the way online advertising firm DoubleClick collects user information." [4] According to the report, the company may be collecting sensive data about consumer purchases through its ad-serving technology. Companies who contract with DoubleClick for advertising services may be violating their own privacy policy without even know it by using DoubleClick. This complaint follows a similar filing by the Electronic Privacy Information Center. There were already six lawsuits, some of which are of class-action status, against DoubleClick, when this complaint was filed. DoubleClick explained the purpose of this linking differently. According to them, the plan to track consumers' movements online and to attach that data to people's real names and addresses is "to better target advertisements to consumers as they surf the web." [5]

More recently, in March of 2001, Richard Smith, chief technology officer at the University of Denver's Privacy Foundation briefed the congressional privacy caucus on web bugs.

> Senator Richard Shelby, R-Ala., said he was outraged at the sophistication of some new generations of bugs, which can secretly extract the sensitive data from a user's computer while they are visiting a web site .... You can get more information off a computer than through a wiretap .... Shelby said Web bugs cab steal the most sensitive information on a computer hard-drive, leaving no trail of lost data and giving the computer user no knowledge of what the Web bug operator has been doing .... Gary Clayton, chief executive officer of the Privacy Council, show lawmakers how Web bugs can be used to extract data from a computer within minutes of logging onto a Web site, without a computer user's knowledge.
>
> The Privacy Council is not associated with the Privacy Foundation.
>
> In the demonstration, Clayton's address book with 1,800 phone numbers and addresses and a congressional memo were taken from his computer ... [6]

So we see that more than just IP address and date/time information can be gotten without a persons knowledge all because of these invisible gifs. Are these web bugs illegal? Today they are not illegal, but it is still too early for the final say since at least the US government is involved. While the use of web bugs may not be illegal, one thing for certain, their use is certainly controversial. With government representatives becoming more knowledgeable and aware of what is actually being done on the web, we are starting to see that this is much more than the scare tactics of a few privacy crazies. As Richard Smith (chief technology officer, Privacy Foundation, University of Denver) pointed out to the congressional caucus in March of 2001, that he was able to identify four million web bugs placed by thirty vendors on various web sites. These little one-pixel gifs are showing up everywhere:

at online banks
at hotels where you book a vacation stay
at FedEx
and even at Oil of Olay web site.

Is it a wonder that consumers are concerned about privacy issues when purchasing on the Internet?

Web bugs were not directly addressed in a report from Forrester Research when it projected that online retailers could loose $15 billion US dollars, or twenty-seven percent of the projected e-commerce revenues for this year because of consumers' privacy concerns. "Thirty-seven percent of online consumers said they would buy more online if they were not worried about privacy issues." [7]

As security professionals, we need to point out that web bugs can cause loss of revenue. We need to urge a new set of business standards in regards to "cookies" and "web bugs." Only then, when the consumers have regained faith in positive ethical standards will Internet business finally overcome the fears of the consumer. According to Statistical Research, Inc., *SRI Report How People* TM *Use the Internet*, while Internet experience does little to ease concerns regarding the loss of privacy, there are a few relatively simple steps a business can take to greatly allay consumers fears:

guarantee against credit card fraud
display their privacy policy prominently
do not sell or share personal information and make this known to consumers
minimize use of cookies that track consumers' Internet activity

In addition, privacy policy must be made more succinct and easier to read. According to the Privacy Leadership Initiative, a trade group including IBM, Dell Computer, DoubleClick and some of the nation's largest credit reporting agencies, web-savvy browsers almost never bother to read privacy policies. Only three percent of more than two thousand adults in a recent survey said that they bothered to read privacy notices carefully, and nearly sixty-four percent said that they did not read the notices at all, or only glanced at them. More than seventy percent said that they would prefer shorter versions such as a check list of privacy promises. [8]

If web bugs are used, then their use must be disclosed in a business's privacy policy. It must be clearly stated exactly what the web bugs are used for. Businesses must insure that any company contracted with must also follow the contracting company's privacy policy. Then comes the hardest part, businesses must verify and review periodically to make sure that the policy continues to be followed by all parties involved.

There are companies who are listening. AOL Online has recently changed its privacy policy to clearly state it's use of web bugs and how they will be used:

> **Information About All AOL Anywhere Visitors** In general, our site automatically gathers certain usage information like the numbers and frequency of visitors to AOL Anywhere and its areas, very much like television ratings that tell the networks how many people tuned in to a program. We only use such data in the aggregate. This aggregate data helps us determine how much our customers use parts of the site, so we can improve our site to assure that it is as appealing as we can make it for as many of you as possible. For example, AOL Anywhere uses a technology nicknamed "cookies" that tells us how and when pages in our site are visited, and by how many people. These cookies do not collect personally identifiable information and we do not combine information collected through these cookies with other personally identifiable information to tell us who you are or even what your screen name or e-mail address is. We also may provide statistical "ratings" information, never information about you personally, to our AOL Anywhere partners about how our members, collectively, use AOL Anywhere. We do this so they too can understand how much people use their areas and our site in order for them to provide you with the best possible Web experience as well. Finally, AOL Anywhere, its advertisers and ad servers may also use cookies, as well as small pieces of code called "web beacons" or "clear gifs," to determine on an anonymous basis which advertisements and promotions users have seen and how users responded to them, but do not use these technologies to collect personally identifiable information unless you give us permission to do so. [9]

This is a huge step in the right direction. What can be done to protect the consumer until all companies change their policies and their habits? There are tools, some free, that can help us identify and/or block web bugs. One free tool, Bugnosis, created by the Privacy Foundation, is a web bug detector that makes web bugs visible. This application does not stop web bugs from doing whatever they were created to do, but it lets the browser know when one is found on a web page and displays the hidden web site. For additional information see: http://http://bugnosis.org

To eliminate web bugs so that they cannot touch your hard drive without first being acknowledged and accepted by you, there are other products. One of these filtering products is WebWasher which is designed to block cookies, web bugs and referer strings. This is a free tool to home users, schools and public educational facilities. There is also an Enterprise Edition that protects the privacy of corporate computers in much the same fashion, with additional enhancements. For more information, see: http://www.webwasher.com

And so we find that we have indeed traveled into a truly "brave new world." Like Winston Smith, we are being watched by "Big Brother" in the form of these little one-pixel gifs called web bugs. nd We are rebelling against the "New World Order" again just as Winston Smith does. Now you know what they are, how they work, what they can do and how to stop them. The task I leave you with is to remain ever vigilant in your push for strong ethical standards, for clear and understandable privacy policy and for continued review that your enterprise is abiding by your our policy. Only by your eternal vigilance will we escape the clutches of "Big Brother" and find freedom in the truly "Brave New World."

Footnotes:

[1] Richard M. Smith, "FAQ:Web Bugs," http://www.privacyfoundation.org/resources/webbug.asp#1 , date not given.

[2] "Web Bug Basics ... Advanced," (The Privacy Foundation), (http://www.bugnosis.org/faq.html#web%20bug%20basics , date not given.

[3] "Web Bug Growth Fuels Privacy Debate," (Cyveillance, Inc. Press release), http://www.nua.ie/surveys/index.cgi?f=VS&art_id=905357096&rel=true , Aug. 14, 2001.

[4] Jim Hu, "Consumer group blasts DoubleClick in report to FTC," http://news.cnet.com/news/0-1005-200-1561502.html , March 1, 2000.

[5] Ibid

[6] Lance Gay, "Technology: Web bugs secretly track users, extract information, privacy advocates say," http://archive.nandotimes.com/technology/story/0,1643,500458962-500698574-503789316-0,00.html , March 2, 2001

[7] "Forrester Research: Privacy issues inhibit onlne spending," NUA Internet Surveys, http://www.nua.ie/surveys/index.cgi?f=VS&art_id=905357259&rel=true Oct. 3, 2001.

[8] "Harris Interactive: Website privacy policies need plainer English," NUA Internet Surveys, http://www.nua.ie/surveys/index.cgi?f=VS&art_id=905357471&rel=true , Dec. 4, 2001.

[9] "Privacy Policy," (AOL Anywhere), http://www.aol.com/info/privacy.html , November 20, 2001.

Additional References:

"WebWasher product sheet," WebWasher AG, Http://www.webwasher.com/product_pdf/english/Product_sheet_WebWasher.pdf , date unknown.

"Web Bug Report," E-Soft, Inc., Http://www.securityspace.com/s_surveys/data/man.200102/webbug.html , March 1, 2001.

Stefanie Olsen, “Nearly undetectable tracking device raises concern,” Http://news.cnet.com/news/0-1007-200-2247960.html , July, 12, 2000.

“AOL says hi to Web bugs,” http://www.geek.com/news/geeknews/2001oct/gee20011008008227.htm , October 28, 2001.

Jim Hu, “AOL is keeping an eye on you,” http://www.zdnet.com/zdnn/stories/news/0,4586,5097903,00.html , October 5, 2001.