Web Beacons – Guidelines for Notice and Choice

The following statement was developed by a coalition of companies[1] in an effort to guide the appropriate use of Web Beacons.[2] The coalition is made up of companies from a broad range of industries.

The coalition of companies responsible for these guidelines believes that Web Beacons are important tools. However, without broader consumer understanding of the technology and data practices involved, Web Beacons will continue to engender confusion and misunderstanding. As such, it is paramount that industry provides clarity regarding the use of these tools.

These guidelines are designed to address consumer concerns regarding the use of Web Beacons by educating businesses about the purpose of Web Beacons and the appropriate provision of notice and choice when Web Beacons are being used. Further, it is anticipated that the notice and choice standards described in these guidelines will result in greater consumer acceptance of Web Beacons as a tool that, when appropriately used, can provide important benefits to the online economy.

While these guidelines provide appropriate standards for notice and choice when Web Beacons are used, they do not address the other Fair Information Practice principles of access, security and enforcement. These guidelines are designed to reside within the broader protections of a web site's privacy policy and existing privacy seal programs (such as TRUSTe and BBB Online). Within the framework of these broader protections, the other Fair Information Practice principles are addressed.[3]

[1] The following companies participated in the development of these guidelines: 24/7 Realmedia, Advertising.com, Atlas DMT, an operating unit of aQuantive, Coremetrics, Doubleclick Inc., Guardent, IBM, KeyLime Software, Microsoft, MundoMedia, the Privacy Council, the US Postal Service, Valueclick, Verizon, Watchfire, and WebSideStory. Two major self regulatory seal programs, TRUSTe and BBB Online, also assisted in this process. The coalition was convened through the administrative support of the Network Advertising Initiative (NAI).

[2] Web Beacons are known by many names. They have been called web bugs, single pixel GIF, pixel tags, smart tags, action tags, clear GIFs, tracers, 1x1 GIFs, and cookie anchors.

[3] The guidelines for the provision of notice and choice when using web beacons are not intended to conflict with the NAI Principles for Online Preference Marketing (OPM). If a conflict between these guidelines and the NAI Principles emerges, the NAI Principles shall control.

Web Beacon Statement Overview

1. Any use of Web Beacons, whether through a website or email, requires notice.

2. Notice must include a disclosure that Web Beacons are being used; the purpose for which the Web Beacons are being used; and, if applicable, a disclosure of any transfer of data to third parties.

3. Organizations that use Web Beacons to transfer Personally Identifiable Information to a Third Party, for purposes unrelated to the reason for which the Personally Identifiable Information was initially collected, must provide choice for such transfers.

4. Organizations that use Web Beacons to transfer sensitive information associated with Personally Identifiable Information to a Third Party must obtain explicit consent (opt-in) for such transfers.

Web Beacons Today

Web Beacons are an integral tool on the web today. In their simplest form, Web Beacons are small strings of code that provide a method for delivering a graphic image on a web page or in an email message for the purpose of transferring data. For example, when an Internet user visits a page on a website, the code for a page being visited may include instructions to go to another server to gather a single pixel graphic image (a Web Beacon). The server providing this Web Beacon may be controlled by the same party as the website being visited, or by another party that has been given permission to place the Web Beacon on the site. Frequently, the Web Beacon is designed to blend into the background of the page being visited.

Web Beacons can be as simple as the example provided above. The purpose of the Web Beacon may be to merely generate a “log file” record on the website’s or Third Party’s server. This may allow websites to better understand usage patterns and some limited characteristics about site visitors (for example, the types of operating systems being used by visitors).

Web Beacons can also be used to deliver cookies or downloadable applications. In these situations, the code for the site being visited includes the same instruction to go to another server to fetch a small graphic file. However, instead of simply delivering the graphic file, the other server may also deliver a cookie or downloadable application. In this manner, the other server (which may be controlled by the site itself) may use cookies to recognize a single browser

across a number of domains or sites. Again these actions may be accomplished by the website itself, an Agent, or a Third Party. In all cases, the use of Web Beacons requires the acceptance of the website being visited. This is because a Web Beacon must be added directly to the code of the website being visited.

Businesses may use Web Beacons for many, many purposes – including site traffic reporting, unique visitor counts, advertising auditing and reporting, and personalization. These tools are critical to the current functionality enjoyed by all on the web today:

- Web Beacons allow sites to better understand the traffic patterns within their domains and, subsequently, adjust their content to better respond to their visitors' interests.

- Web Beacons allow advertisers to understand the response patterns ("conversions") in online advertising. This allows advertisers to tune their marketing campaigns to ensure optimal effectiveness.

- Web Beacons allow e-commerce sites to recognize the visitors generated from online and email advertising campaigns. In this way, e-commerce sites can tailor the content presented to such visitors to maximize the branding and marketing effect of their campaigns.

- Web Beacons allow websites to create standardized reporting tools for the numbers of unique visitors that flow through their sites. In this manner, sites can distinguish between a visitor that hits a single page on their site and visitor that may hit 30 pages on their site.

- Web Beacons allow email marketers to monitor users' readership levels so that they can identify aggregate trends and individual usage to provide their customers with more relevant content or offers. They may recognize activities such as when the e -mail was opened, how many times a message was forwarded, which URLs were clicked, some information about the message in which the URL was found, and the actions taken by a visitor on the marketer's website after clicking on a URL.

A significant majority of online Web Beacons are used to collect only anonymous data and not data such as name, address or email. This is true, regardless of whether the Web Beacon is being served to generate a log file record, serve a cookie, or download an application.

Some Web Beacons may be used to collect Personally Identifiable Information. This may be particularly true in the case of email that contains a Web Beacon. In such cases, the data collected through the Web Beacon may be linked to the recipient's email address or other information identifying the recipient.

Ultimately, Web Beacons provide us with an online tool that enables many of the services and features Internet users enjoy on the web today. Without Web Beacons, websites would have much less ability to understand the traffic patterns – and therefore the interests and needs – of their visitors and customers. Advertisers would lose their ability to recognize effective ad campaigns – and would therefore be less inclined to spend limited marketing resources on online media. Without Web Beacons, consumers would immediately notice a significant decrease in the functionality of the web. As such, Web Beacons remain an important and helpful tool in the online economy.

Web Beacons provide further benefits to consumers by allowing e -commerce to standardize and understand the dynamics of online marketing. Web Beacons give marketers significant detail regarding the effectiveness of their advertising campaigns. Providing this level of detail results in a greater willingness to invest advertising dollars in online media (web sites). And continued spending in online media supports the vast diversity of free content and services that consumers enjoy online today.

Definitions Used in These Guidelines

FIRST PARTY (Collector) – means that the Web Beacon is being delivered by the Organization responsible for the website being visited. “Organization” means the entity responsible for the site being visited and includes any Affiliates of such entity, all of which have a substantially similar privacy policy associated with the use of the Web Beacon. “Affiliate” means any organization that controls, is controlled by, or is under common control with another organization.

AGENT (Processor) – means that the Web Beacon is being delivered by an Agent for purposes exclusively related to the needs of the First Party. In this context, the contract between the First Party and the Agent must clarify that the Agent cannot use any individual, non-aggregated data gathered through the Web Beacon for its own purposes. In other words, the data is still “owned” by the First Party. The use of anonymous data by the Agent for aggregate or statistical purposes does not constitute a use for the Agent’s purposes.

THIRD PARTY – means that the Web Beacon is being delivered by a Third Party and that the Third Party gathers data through the Web Beacon for its own purposes. In this situation, the Third Party may be providing services to the First Party. The distinction lies in the subsequent use of the data by the Third Party. In this context, the Third Party should have contractual rights to the data.

PERSONALLY IDENTIFIABLE INFORMATION (PII) -- means data that can be used to identify or contact a person, including name, address, telephone number, or email address. PII also includes any other data, such as, but not limited to, anonymous identifiers, demographic or behavioral data, when such data is linked

to PII and identifies a person to the party holding such data. Data that is PII for one party may not constitute PII for another.

WEB BEACON—Generally, a Web Beacon consists of a small string of code that represents a graphic image request on a web page or email. There may or may not be a visible graphic image associated with the Web Beacon and often the image is designed to blend into the background of a web page or email. Web Beacons may be delivered from the same or a different domain than the web page or email being viewed. Web Beacons may be used by the party responsible for the web page or email being viewed (First Party Web Beacons) or by third parties (Third Party Web Beacons).

Web Beacons – Guidelines for Notice and Choice

Any use of Web Beacons requires NOTICE. In some cases, the use of Web Beacons will also require the provision of CHOICE.

NOTICE – Whenever Web Beacons are used on a website, the privacy policy for the site must include notice of the use of Web Beacons. The privacy policy of the site must be available from, at a minimum, the main page of the site and, in addition, every page from which information gathered through a Web Beacon either contains or is linked to PII. The link to the privacy policy should be clear and conspicuous. For email messages that include a Web Beacon, notice, or a link to a privacy policy that includes notice, must be provided in every email that includes a Web Beacon. In all situations, the Web Beacon notice must include:

1. A disclosure that cookies and/or Web Beacons are being used;

2. A disclosure of the purpose for which the Web Beacons are being used;

3. A disclosure, if applicable, of whether Personally Identifiable Information is linked to the Web Beacon;

4. A disclosure, if applicable, of any transfer of data collected through the Web Beacon to Third Parties; and

5. A disclosure, if applicable, that Agents or Third Parties may be using Web Beacons in the email or on the site.

CHOICE – Visitors to a site or recipients of an email must be afforded a choice over data transfers through Web Beacons in those situations where Personally Identifiable Information is being transferred to a Third Party[4]. Such choice must be available through the site's privacy policy or at the time and place where the PII is being gathered. Choice is not required when Personally Identifiable Information is being transferred to a First Party or an Agent. Prior to a transfer, individuals must be afforded an opportunity to explicitly consent ("opt-in") to those situations where a Web Beacon is being used to transfer to a Third Party Personally Identifiable Information linked to sensitive information[5].

A NOTE ABOUT P3P AND THIS STATEMENT: The growing use of the Platform for Privacy Preferences (P3P) is an important step in the protection of consumer privacy. The companies responsible for these guidelines encourage all online organizations to review the P3P specification and consider implementation. It should be noted that implementation of P3P statements on websites and cookies is not sufficient to satisfy the notice requirements described in this document. Under the guidelines created within this document, notice must be provided through a site's (human-readable) privacy policy.

[4] Choice may be offered in the form of an "opt-out" (implied consent) or an "opt-in" (explicit consent) depending on the jurisdiction and the business practices of the organization involved. At a minimum, visitors must be offered the opportunity to opt-out of transfers to Third Parties of PII through the use of Web Beacons.

[5] Sensitive information is defined by many laws and regulations in various ways and may include various forms of data – including certain types of health, financial, sexual and political data. This document does not define sensitive information. Rather, organizations are encouraged to refer to applicable laws regarding sensitive data in their jurisdiction.