Comments of the Global Privacy Alliance on Cookies and Web Beacons

September 2010

Comments of the Global Privacy Alliance on Cookies and Web Beacons

Comments of the Global Privacy Alliance[1] on Cookies And Web Beacons

I. Introduction

The Global Privacy Alliance ("GPA") is pleased to offer this white paper on the technology and common uses of cookies and Web beacons and our recommendations on how cookies, in particular, should be regulated. Our recommendations on cookies regulation is in response to the invitation extended to industry in Opinion 2/2010 on online behavioral advertising by the Article 29 Working Party. As EU Member States begin to transpose the amendments to the ePrivacy Directive set forth in Directive 2009/136/EC into national law, and in relation to the review of the general EU data protection framework, government policymakers and legislators should have a clear understanding of how the technology is used in practice. Moreover, we think it is instructive to consider the challenges faced by US policymakers as they consider how best to promote a robust electronic marketplace while at the same time ensuring that the privacy interests of Internet users are sufficiently protected. All policymakers should exercise caution when attempting to regulate these technologies because it is impossible at this early stage to foresee the impact such regulation might have and, in particular, the unintended consequences that could result from a rush to regulate this dynamic marketplace.

Recommendations

In June 2010, the Article 29 Working Party issued an opinion on online behavioral advertising to clarify the applicable legal framework, particularly with respect to advertising network providers and their use of Third Party cookies. While the Working Party acknowledges the economic benefits that behavioral advertising brings to some stakeholders, we believe that its proposed approach could be further strengthened by encouraging greater transparency on the Web. Otherwise, the growth of the Internet marketplace might be adversely affected.

---

[1] The Global Privacy Alliance ("GPA") is comprised of a cross section of global businesses from the financial services, automobile, aerospace, consumer products, computer and computer software, communications, and electronic commerce sectors. The GPA works to encourage responsible, global privacy practices that enhance consumer trust as well as preserve the free flow of information. Members of the GPA take their privacy obligations very seriously. The views expressed herein generally represent the views of the members of the GPA. While all members support the overall approach presented in this paper, some of the individual points raised may not be relevant to all members.

In relation to any regulation on cookies, we would like to submit the following concepts and recommendations for further consideration:

- **Need for a Nuanced Approach:** EU Member States could consider adopting a more nuanced and flexible approach. Such approach might involve a mixture of enhanced notice and opt-out where necessary, and appropriate and certain instances of opt-in, narrowly tailored to protect consumers' privacy interests where they are most likely to be threatened. Member States would thus further contribute to better consumer protection, while preserving innovation and the continued growth of the Internet.

- **No Blanket Opt-In Standard:** Member States might consider refraining from adopting a blanket opt-in requirement for all uses of cookies and similar tracking technologies. Under the current framework, there is a clear distinction between the use of sensitive data and other personal data. Applying the opt-in standard currently in place for sensitive data to the use of not obviously identifiable data would be excessive. This would lead to an inflation of click-though consents. Users will be overburdened and would fail to recognize when sensitive data are in play. Rather, the current distinction should be preserved, while improving on greater transparency, *e.g.*, through the use of an icon in or around behaviorally targeted advertisements, resulting in a recognizable notice and an easy-to-find and easy-to-use means of opting out.

- **Distinguish between Primary and Secondary Uses by Data Controllers and Processors:** Member States could explore the possibility of implementing an approach that distinguishes between different types of uses and does not treat all uses in the same way. In particular, "primary uses," those uses for which the user provided the data or that are obvious to users under the circumstances, should be treated differently from other types of uses ("secondary uses"). Users inherently understand that when they directly interact with a Website or business that they then are likely to receive targeted communications from that business.[2] Secondary uses, however, are not likely to be obvious to the user and consequently, should be treated in a different manner. Therefore, the type of choice offered to an individual should be tailored to the individual's reasonable expectations under the circumstances.[3] The Working Party seems not to recognize

[2] The Federal Trade Commission has acknowledged this point. *See* FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising, at 26-27 (February 2009) (Final FTC Report and Principles), *available at* http://www2.ftc.gov/os/2009/02/P085400behavadreport.pdf.

[3] The FTC Chairman articulated this principle in his testimony before the US Congress. *See* Prepared Statement Of The Federal Trade Commission On Consumer Privacy Before the Committee On Commerce, Science, And Transportation, United States Senate (July 27, 2010), at p. 22 ("Leibowitz testimony"), *available at* http://www.ftc.gov/os/testimony/100727consumerprivacy.pdf.

the distinction in its opinion and does impose the opt-in requirement to on-site behavioral advertising when a user visits a site, and the operator of that very site tracks the online behavior.

- **Enhanced Notice and an Opportunity to Opt-Out For Secondary Purposes:** For secondary uses, Member States might consider an approach that requires an enhanced notice, and provide a clear, easy-to-find and easy-to-use opportunity to opt-out. The concept of "enhanced notice" could prompt the business community to develop a new standard for transparency and thereby enhance consumer control and protection, as has been the case in the US.

- **Default Opt-In for Secondary Uses of Sensitive Data:** For the collection of sensitive data for a secondary purpose, explicit user consent is considered appropriate.

- **Importance of Harmonization at the Member State Level:** Harmonized implementation at the Member State level is key to fostering greater consumer protection and preserving innovation and the continued growth of the Internet. Any variation in regulations across the Member States could have a chilling effect on this dynamic marketplace.

US Regulatory Model: Overview of Lessons Learned

The above recommendations are based on the lessons learned from cookie regulation in the United States. The GPA believes that the US approach so far has provided a number of benefits, including raising awareness of privacy as a core value for business, allowing industry to develop a very promising and flexible regime, while making clear that certain activities, such as the use of sensitive information for behavioral advertising, should require consumers' affirmative, opt-in consent (this is one of the principles the US Federal Trade Commission ("FTC") set forth when it established a framework for industry).

Therefore, it could be useful for the EU Member States to draw inspiration from this experience and implement a similar approach in their respective jurisdictions.

Businesses worldwide have been deploying cookies for a variety of purposes since 1994, when cookies were first introduced by Netscape. From then on, the FTC and the US Congress have been active in developing appropriate ways to regulate uses of cookies that balance the interests in promoting innovation, allowing for a user experience that is consistent with users' expectations, and protecting the privacy interests and rights of users.

The US experience with cookie regulation has revealed a number of core principles: the consideration of unintended consequences of regulation in terms of stifling innovation, and causing economic harm; the development over time of a hybrid approach to the types of notice and consent that should be required, depending on the context; and a recognition that it is inherently difficult to change regulation at a pace that is consistent with the speed of technology innovation. Thus, a trend toward promoting self-regulation, backed by the threat of regulation if self-regulation fails, has emerged, with enforcement actions in egregious cases. This approach has led to the development of an industry-promoted program that will deploy an icon in or around behaviorally targeted advertisements, resulting in a recognizable notice and an easy-to-find and easy-to use means of opting out, meaning a possibility to object to the use of cookies by a certain advertiser.

The GPA believes that the United States approach so far has provided a number of benefits, including raising the awareness of privacy as a core value for business, allowing the industry to develop a very promising and flexible regime, while making clear that certain activities, such as the use of sensitive information for behavioral advertising, should require consumers' affirmative, opt-in consent (this is one of the principles the FTC set forth when it established a framework for industry). We think the model is working well in the United States, and therefore recommend that the EU Member States consider implementing a similar approach in their respective jurisdictions.

II. Overview: Cookies And Web Beacons – Underlying Technology, Key Users, and Common Uses

This section explains the technology behind cookies and Web beacons, who uses them and why.

A. Cookies

What is a Cookie?

A cookie is a text file, typically no more than four kilobytes in size, stored on a user's computer by the user's browser. The purpose of cookies is to allow a Website to recognize a user when he or she makes multiple visits a website, or separate pages in a Website. When a user requests a Web page, for example, by typing www.example.com into his browser address bar, the page's server responds by delivering the requested page and may request the browser to store cookies. The user's browser will store a cookie if it is configured to support cookies. If the user's browser does store cookies, then as the user visits the site, by linking to any of the Web pages or adding items to the Website's shopping cart, for example, the cookie initially placed on the user's computer will be read

by the site and additional information may be recorded on that cookie based on the user's activity on the Website. This way, the server is able to recognize the user and track his or her activity on the site.
Cookies placed on a user's computer by a site can generally only be read by the domain that set them.[4] For example, www.example2.com can read cookies that it sets on users' browsers when users visit that site, but cannot read cookies set by www.example3.com when the user visits www.example2.com.[5]

Users benefit in tangible ways from cookies. For example, cookies perform an important authentication function. Cookies may be used by website operators, such as banks or retailers, to recognize users when they return to the Website. Users only need to log in with their username and password, after which the Website will set a cookie that identifies the user. As the user navigates the site, each page within the site will confirm the login credentials by checking the cookie. While many sites set these cookies to terminate at the end of the browsing session, other sites allow the user to elect to be "remembered" when they login in the future. When users make this selection, the Website will change the cookie to be persistent over multiple browser sessions.

Cookies also enable users to personalize the website to suit their individual needs, such as setting their language preference to English or some other language. In addition, parents can use cookies to protect their children online, by setting and maintaining browser preferences that will filter out online searches for pornographic or sexually explicit content, blasphemous or other types of content inciting hatred.

Without cookies, the Internet becomes "stateless," or "forgetful": each request for a Web page from a user's browser is treated separately from every other request. Consequently, users would not be able to enjoy the many benefits that they experience today (and expect) whenever they go online.

Persistent vs. Session Cookies. There are two types of cookies: persistent and session. Session cookies are typically not stored on the user's hard drive, and they cease to exist at the end of the browser session. Persistent cookies, on the other hand, are stored on the user's hard drive and remain active beyond a single session on a browser.[6]

---

[4] Cookies can be set at either the site or domain level. A domain may host multiple sites. So, for example, if cookie is set at the domain level (*e.g.*, www.example.com) and there are multiples sites located on that domain such as www.investorrelations.example.com and www.intra.example.com, then these sites will be able to read that cookie. However, if the cookie is set at the site or subdomain level, for example, by www.intra.example.com, then www.investorrelations.example.com or www.example.com will not be able to read www.intra.example.com's cookie.

[5] The domain owner can, however, configure his or her Domain Network System (DNS) to allow a Third Party to use one of his subdomains. The Third Party will then be able to share certain cookies with the domain owner.

[6] The domain that sets cookies causes them to be persistent across different online sessions by specifying an expiration date. The cookie is deleted from the user's hard drive on that date. If the domain that sets the

What Information is Stored in a Cookie?

Cookies can contain any type of information, but only in limited amounts. For example, they are often used to store a username and password for a Website, so that a user who registers once does not have to log in every time they access the Website. They can also store shopping cart contents, users' preferences and other data used by Websites, for example, to track one request to the next.

A browser stores a cookie on the user's computer in the same way that a user stores a Microsoft Word document on his or her computer. Microsoft Internet Explorer, for example, will typically store cookies as separate files in C:\Documents and Settings\<username>\Cookies. (Different browsers on the same computer may use different cookie files.) *Cookies are not programs and do not execute any functions or perform any tasks*.

Since many cookies are typically no larger than four kilobytes[7] some sites use cookies to store a simple, unique, anonymous identifier, called a "Cookie ID" or a "reference ID," and then store other cookie-related information on their servers. When a user visits their site, they use the reference ID contained in the user's cookie to link that user with more meaningful amounts of information stored on their servers.

Nearly all servers store the following information for every cookie request:

- Cookie ID
- IP Address
- Date/Time Stamp
- What was requested
- Referring URL
- Status of request (okay, redirect, etc.)
- Size of requested asset in bytes
- Authenticated user (optional; only appears on sites where user name/password is required)

Who Sets Cookies?

---

cookie does not specify a date, then the cookie is deleted at the end of the user session (when the user exits the browser). For example, an e-commerce Website may use persistent cookies to store the items users have placed in their shopping cart. This way, if users exit their browser without making a purchase and return to the Website later, they will still find the same items in the cart so they do not have to look for these items again. If these cookies were not given an expiration date, they would expire when the browser is closed, and the information about the cart content would be lost.

[7] http://www.informit.com/articles/article.aspx?p=31842&seqNum=4.

Cookies can be set by two different types of entities: the Website that the user is visiting ("the First Party," or Website owner/publisher) or a third party such as an ad network provider entity ("the Third Party," or ad network providers).[8] There is no technical difference between the cookies set by these entities. The cookies simply belong to different entities.

How Can Browser Settings Be Used To Exercise Choice With Respect To Cookies?

All major browsers offer users the following basic controls:

(i) accept all cookies;
(ii) block all cookies;
(iii) prompt for all cookies;
(iv) accept cookies based on their being First or Third Party;
(v) block all cookies based on their being First or Third Party; and
(vi) prompt for all cookies based on their being First or Third Party.

Some browsers also allow the user to see the cookies that are active with respect to a given page, and some incorporate a cookie manager for the user to see and selectively delete the cookies currently stored in the browser. Most browsers also allow users to perform a full deletion of all personal data, including cookies. Add-on tools for managing cookie permissions also exist. Thus, users are afforded control over cookies, by both browsers and software providers, at a level of granularity that can be tailored to suit their individual comfort levels.

B. Web Beacons

What is a Web beacon?

A Web beacon is an object, usually invisible to the user, that is embedded in a Web page, advertisement, or an e-mail. Also called Web bugs, pixel tags, and clear GIFs, Web beacons are used together with cookies to help Websites understand the behavior of their customers as they visit the site. They are usually 1 pixel x 1 pixel in size. Generally, Web beacons do not store information on the user's computer.

Web beacons are typically used to monitor and record the activity of a site. For example, when a user visits a Web page, the page may contain code that redirects the user's

[8] Cookies can also be set by agents or service providers hired by the Website owner/publisher to act on its behalf; however, these entities are under the control of the Website owner and are acting on its instructions only. Consequently, such agents or service providers should be treated as a First Party in this context.

computer to go to another server to gather a Web beacon. The server providing the Web beacon may be controlled by the First Party (the Website owner or its agent) or by a Third Party (the network advertiser) that has been given permission to place a Web beacon on the site.[9] The Web beacon can be used to generate a "log file" record on the Website's or Third Party's server which will enable the Website to better understand usage patterns and some limited information about visitors to their site (such as their type of operating systems). Web beacons can also be used to call a server to set cookies. Cookies placed by this other server will enable it to recognize the user's browser across a number of domains or sites. If the user sets his or her browser to reject all cookies, the Web beacon will not be able to track the user's specific activity but it may still record an anonymous visit from the user's IP address. [10]

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 or to serve a cookie. Some Web beacons, however, 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 e-mail address or other information identifying the recipient.

The e-Privacy Directive does not cover Web beacons; its Article 5(2) refers only to terminal equipment of the user, thus the purpose of the information provided in Section II of this paper should be seen only as necessary clarifications aimed at facilitating the distinction between various tracking technologies. The intention of such an inclusive approach is to provide a more coherent perspective on the complex and interconnected nature of tracking technologies. The following reflections concerning cookies are therefore complemented by additional information concerning Web beacons. It should be understood, however, that both technologically and legally, Web beacons cannot be equalized with cookies. Consequently, the recommendations proposed in Section III of this paper concern only cookies.

C. How Are these Technologies Used and Who Uses Them?

Cookies

---

[9] Agents of the Website owner may only use Web beacons for purposes exclusively related to the needs of the Website owner and may not use individual, nonaggregated data for its own purposes. In contrast, Third Parties may use the Web beacons for the purpose of providing services to the Website owner but usually also have contractual rights to use the data for their own purposes. *See* the NAI Web Beacon Guidelines, available at http://networkadvertising.org/networks/Web_Beacons_rev_11-1-04.pdf.

[10] *See* the NAI Web Beacon Guidelines.

Cookies are used for many different and useful purposes. In particular, cookies are used to authenticate users on Websites, store their site preferences and shopping cart contents, improve the user's ability to navigate the site, deliver targeted advertising, and conduct site analytics and research. As discussed in greater detail below, cookies can be set by two different types of entities: the First Party (the Website owner or its agent) or the Third Party (a network advertiser).

First and Third Party Cookies

When a user views a Web page, he or she will typically see images and other objects that reside on the Website's server as well as images (*e.g.*, advertisements) and other objects that are visible from the Website but reside on a different Web address or Url. The user's browser downloads all of these images and objects (widgets, advertisements, etc.). While they are retrieved, some of them may set cookies in the user's browser. First Party cookies are set by the same domain that the user visits. Third Party cookies, on the other hand, are set or returned from different domains.

By way of example, a First Party cookie would be used by an e-commerce Website to recognize users when they return and to offer recommendations for products or services based on their previous transactions on the Website, or on what others who exhibited similar behaviors on the site may have done. Thus, users may see a message on a Website reminding them that they have an item remaining in their shopping cart; that based on the books they have purchased, they may like other books; or that based on the music they have purchased, they may be interested in music that other users who have purchased the same music have also purchased.

A Third Party cookie is set by an advertising company with the permission of the Website owner. When visiting a Website, the user may get: (1) a "Website.net" cookie that the Website uses to recognize the user; and (2) an "advertising company.net" cookie. The Website may work with the advertising company to engage in advertising known as "retargeting," whereby, for example, a user who abandons a full shopping cart may receive an advertisement for the same items in the shopping cart on other Websites he or she visits at another time.

Because the site controls the content served on it, Third Party cookies appear only at the site's request or with its permission.[11]

---

[11] HTML provided by the First Party can contain references to other parties that make their own communications. A "referrer" tells the Third Party which First Party called it. [cnn/advertising.com example] Each entity providing content on the First Party's page has a separate communication/relationship with the user. Each site or domain in the process can read only the cookies scoped to them. Although the First Party site determines what content will be called, it cannot read the cookies used by the other content providers.

Web Beacons

As discussed above, Web beacons are used together with cookies to help Websites understand the behavior of their customers as they visit the site. In particular, Web beacons are for purposes such as site traffic reporting, unique visitor counts, advertising auditing and reporting, and personalization. Web beacons can be placed by the First Party (the organization responsible for the Website), an agent of the First Party, or a Third Party.

Uses of Cookies and Web Beacons

1. Improving Services

Cookie technology allows sites to be more user-friendly. For example, cookies are used for session management, maintaining data related to the user during site navigation (across multiple visits if the cookie is persistent). This allows the site to remember information about the user, including the contents of his or her shopping cart and his or her registration or preference information. The server encodes this information in a cookie and returns it to the browser, so that every time the user accesses a page of that site the server is also sent a cookie where the preferences are stored and can personalize the page according to the user's preferences.

Similarly, Web beacons allow e-commerce sites to recognize 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.

2. Analytics Using Data Processors

Cookies and Web beacons are often used to conduct site analytics and research. For example, if a user requests a page of a certain Website, and the Website employs an analytics company, the analytics company will have set a Web beacon on the page. The beacon calls the analytics company's server, which either sets a cookie for the first time on the user's hard drive or reads a cookie that it previously set. From this point on, the cookie will be automatically sent by the browser to the server every time a new page from the site is requested. The server will send the page as usual, but it will also store the URL of the requested page, the date/time of the request, and the cookie in a log file. By looking at the log file, the site knows which pages the user has visited and in what sequence.

This technology helps a company measure the effectiveness of its Website, its advertising, and its email in various ways. For example, Web beacons, working together with cookies, can count the number of users who visit a particular site page, who visit a site from a banner advertisement on a Third Party's site and subsequently do or do not

make a purchase, and who open or take other action with respect to an email (such as forwarding or clicking through it). All of this usage information helps a company understand the traffic and response patterns on its site and the effectiveness of its online advertising campaigns. Armed with this information, they can better fine tune their advertising campaigns and adjust the content of their site and/or products to better respond to their visitors' interests.

Analytics companies typically operate as agents for their Website clients. As such, they keep the data they collect for each client separate from data they collect for other clients, and use the data only for their client's purposes. These tools are critical to the current functionality enjoyed by all on the Web today.

3. Reporting

Cookies and Web beacons permit advertisers to measure the reach and efficacy of their advertising and e-mail campaigns, by counting the number of individuals who view and/or take action with respect to an advertisement or email (such as clicking through it or determining if an email has been forwarded).

Web beacons in particular allow advertisers to understand the response patterns or "conversions" in online advertising, allowing them to fine tune their marketing campaigns. In addition, Web beacons allow sites to create standardized reporting tools for the number of unique visitors to their sites. In this way, sites can distinguish between a visitor who visits a single page on the site and one who may visit 30 pages on the site.

4. Marketing

First Party Use

The most common forms of First Party cookies to engage in advertising are ubiquitous on the Internet today. Their core value lies in recognizing a user across page views and browsing sessions in order to offer that user an advertisement or marketing message that is tailored to his activity. Thus, for example, users who shop online may see an advertising message that says something like "users that purchased these books also bought those books."

Third Party Use

In the online advertising world, cookies and Web beacons often work as follows: A user visits Website A, which is a publisher site that allows advertising. The Website allows an advertising services company, Ad Network A, to place a Web beacon on the page, so that when the user visits the page, the Web beacon calls Ad Network A to request an image. Ad Network A's server will also check to see if it has previously set a cookie on the browser of the visitor. If it has, the server may update the cookie with information

associated with that visit, such as the URLs accessed within the Website. If it has not, the server may set a new cookie on the user's browser.

When the user returns to that particular Website, the same process takes place, and Ad Network A's server recognizes the cookie it previously set on the consumer's browser and determines whether the information stored in that cookie (or on the server and associated with the cookie ID) corresponds to a particular advertising segment, such as women's shoes.

Using this example, Ad Network A then would determine whether it has any advertising clients in the women's shoes category. If so, Ad Network A, which previously purchased banner space on the publisher's Website, delivers the women's shoes advertisement into that banner space while the user is on the Website.

The result is that the publisher is able to sell its banner space at a premium because the advertiser knows its ads will only go to consumers who have already expressed an interest in that category of products or services (in this case, shoes). The publisher does not know to whom the advertisement is delivered. The Ad Network only knows that the ad was delivered to a specific cookie ID associated with segments of likely interest based on previous online activities. The advertiser only knows that its ads are delivered according to its instructions, *i.e.*, people interested in purchasing women's shoes.

The model can get more complicated, but not in ways that materially affect users' privacy. For example, Ad Network A may have relationships with numerous publishers, put Web beacons on their pages, and get called every time a user visits any such Web page. Ad Network A would then be able to update its cookie during each such visit and develop a more robust view of the user's Web navigation activities. But that only allows Ad Network A to tell its advertisers that it has cookie IDs associated with URL visits that correspond to marketing segments, such as women's shoes, automobiles, travel, etc. In other words, the size of the network simply allows the Ad Network to have a greater variety of advertising categories to offer advertisers. Size does not allow the Ad Network, publisher, or advertiser to somehow triangulate to identify a particular individual. Nor do those parties have any interest in that; all the advertiser wants to do is to target its advertising to cookies belonging to users whose online activity suggest a greater affinity for certain products or services than is expressed by the online population at large.

D. What Are the Benefits To Users And Operators?

Cookies provide benefits to users and site operators alike. From the user's perspective, cookies can make their shopping and site navigation easier and more enjoyable. In particular, cookies can eliminate the need for users to enter their user name and password every time they access the site. They can also make possible the concept of a "shopping

cart" on the site where the user can make or defer purchases until a later date without having to re-enter information unnecessarily. From the perspective of the site owner, cookies enable them to better understand and respond to the interests of visitors to their site.

Similarly, Web beacons make possible many of the services and features that users enjoy on the Web today. Without Web beacons, Websites would be less able 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 their limited marketing budgets on online media. Online advertising supports a vast diversity of free content and services that consumers enjoy online today.

III. Reflections on the Article 29 Working Party Approach

In June 2010, the Article 29 Working Party issued an opinion (2/2010) on online behavioral advertising to clarify the applicable legal framework, particularly with respect to advertising network providers and their use of Third Party cookies. The opinion addressed both the 2002 ePrivacy Directive (Directive 2002/58/EC), and the subsequent amendments enacted in 2009 (Directive 2009/13/EC) which have yet to be implemented into Member States' national laws. While the Working Party acknowledges the economic benefits that behavioral advertising brings to some stakeholders, it states clearly that such activities must not be carried out at the expense of individuals' rights to privacy and data protection. Importantly, it clarifies that the requirements for First Party cookies and Third Party cookies should be different and that it is important to interpret the legal framework in a flexible way by applying only those provisions that are pertinent to the relevant players. The opinion makes clear that the major compliance requirements are imposed on the advertising network provider.

A. Educational Aspect

While stressing a need for greater transparency, the opinion fails to address user information and education, and includes little incentives for industry to ensure greater transparency through the use of icons and other practical tools. The Working Party acknowledges that most users are not sufficiently informed about tracking technologies, yet it fails to tackle this issue directly. Instead, the solution it proposes is to require opt-in consent. However, simply clicking the consent box "Yes" or "No" will do little to educate users about the choices available to them. The focus should be on providing users with useful information to enable them to make informed choices. Consideration should be given, therefore, to the use of icons and enhanced notices or information so that users can make informed opt-out choices.

The Working Party further proposes that browser settings be set to automatically reject cookies. This proposal, however, is problematical because it would cause many Web-sites to cease working. Users would then simply adjust their browser settings to allow all cookies to be accepted.

A more pragmatic and flexible approach has been presented by the UK Information Commissioner's Office,[12] which drew attention to a variety of privacy choices that strike the right balance between privacy protection and functionality. Privacy choices are understood as options that users are given to set Web browsers or Websites, and allow them to exercise a degree of control over how their online data is used. Privacy options allow people to choose whether to accept cookies, whether to keep a record of their previous browsing activity, and whether to retain the information that is required to fill in a form automatically. Therefore, instead of simply assuming that opt-in consent is the best way to address a user's lack of sophisticated knowledge concerning tracking technologies, more attention could be given to developing a variety of nuanced approaches.

B. More Efficient Consumer Protection

In addition, repeated opt-in consent requests will make Internet browsing more cumbersome and likely desensitize and frustrate users. Users today expect and demand a fast and simple online experience; otherwise, they will shop somewhere else. Alternatively, faced with multiple requests for opt-in consent when browsing the Internet, users may ignore the context and simply click "yes" in order to get to where they want to go on the Internet. Consequently, this approach may decrease user awareness and sensitivity, particular when truly sensitive data are in play (*e.g.*, information about health, sexual orientation, children or location data).

The Working Party seems to recognize that the e-Privacy Directive does not require opt-in consent, and consequently calls for opt-in "in every case" for the collection of personal data. The Working Party suggests that opt-in should be obtained for an interim period, to account for users being unaware of default browser settings that accept cookies. However, this lack of awareness would better be tackled by greater transparency. Also, introducing opt-in for an interim period does not seem logical. If Member States decided to implement the Directive by introducing a time restriction for the opt-in consent, it is highly probable that the time requirements could be set differently in various Member States. It would then only hamper the desired necessity of ensuring the coherent and unified level of the implementation of the data protection framework.

---

[12] The recently published "Personal information online, code of practice" at http://www.ico.gov.uk/ebook/ebook.htm.

C. Providing Better Opportunities for SMEs

It is also important to consider the economic impact of adopting an opt-in consent regime for cookies. With an opt-in consent regime, smaller Websites, which represent the primary growth of the Internet, will have trouble selling their advertising inventory for more than the customary cents per thousand impressions. Growth will likely slow, which, in turn could result in consolidation of players in the market. Large publishers, who can sell their advertising inventory for a premium even if it is untargeted, are likely to be unaffected and continue to grow, commanding an ever-increasing market share. Consequently, one of the most important attributes of the Internet – the ability to put the smallest businesses on a level playing field with the largest companies–will be lost.

D. Recommendations

Need for a Nuanced and Flexible Approach
To address the above issues, EU Member States could consider adopting a more nuanced and flexible approach. Such approach might involve a mixture of enhanced notice and opt-out where appropriate and in certain instances, opt-in consents, narrowly tailored to protect consumers' privacy interests where they are most likely to be threatened. We believe that this type of approach would enhance consumer protection, and at the same time, preserve innovation and the continued growth of the Internet.

Maintain The Distinction Between Sensitive and Non-Sensitive Data And Provide Greater Transparency
Under the current EU framework, there is a clear distinction between the use of sensitive data and other personal data. We believe that it makes sense to maintain this distinction with regard to data collected through cookies. Simply applying a blanket opt-in standard for all uses of cookies is excessive and will lead to an inflation of click-through consents. Users will be overburdened and will fail to recognize when sensitive data are in play. Efforts should be made, however, to provide greater transparency, *e.g.*, through the use of an icon in or around behaviorally targeted advertisements, which will result in a recognizable notice and an easy-to-find and easy-to-use means of opting out.

Distinction Between Primary and Secondary Uses
Moreover, in keeping with the concept of maintaining a nuanced and flexible approach, Member States could explore the possibility of implementing an approach that distinguishes between different types of uses and does not treat all uses in the same way. In particular, "primary uses," those uses for which the user provided the data or that are obvious to users under the circumstances, should be treated differently from other types of uses ("secondary uses"). Users inherently understand that when they directly interact with a Website or business that they then are likely to receive targeted communications

from that business. Secondary uses, however, are not likely to be obvious to the user and consequently, should be treated in a different manner.

Enhanced Notice and an Opportunity to Opt-Out For Secondary Purposes
For secondary uses, we recommend that the Member States consider an approach that requires an enhanced notice, and provides a clear, easy-to-find and easy-to-use opportunity to opt-out. In the United States, the concept of "enhanced notice" has prompted the business community to develop a new standard for transparency and consumer control.

Default Opt-In for Secondary Uses of Sensitive Data
For the collection of sensitive data for a secondary purpose, explicit user consent is appropriate.

Importance of Harmonization at the Member State Level
Harmonized implementation at the Member State level is key to fostering greater consumer protection and preserving innovation and the continued growth of the Internet. Any variation in regulations across the Member States could have a chilling effect on this dynamic marketplace.

IV. The US Experience

The approach taken by the United States provides a useful case study in the regulation of cookies. The FTC has tended to favor self-regulation but, at the same time, has made clear to industry that self-regulation must accomplish certain objectives in order for it to remain a viable alternative to regulation. The FTC has also brought enforcement actions when it believed that a company crossed the line into deceptive or unfair practices. Thus the FTC has set out a framework and investigated and brought enforcement actions against organizations that have not behaved in line with that framework. While the FTC has not said so directly, its cautious approach to imposing new regulations in this area reflects a concern about the unintended *yet unknown and unknowable* consequences associated with regulating technology directly, especially in a dynamic market such as electronic commerce. No one knows how many companies would be affected, whether new Websites that rely on cookies for advertising purposes would survive (thereby supporting the continued growth of the Internet), how many jobs would be at stake, and whether a blanket opt-in would affect entire national economies. Accordingly, an approach that balances legal objectives, privacy rights, and a desire not to unnecessarily interfere with the marketplace appears to be warranted.

A. FTC Looks at Behavioral Advertising

In 2009, after two years of thorough examination of behavioral targeting, including public consultation, the FTC Staff issued an unanimously approved report entitled "FTC

Staff: Principles for the Self-Regulation of Online Behavioral Advertising" ("Final Report and Principles").[13] The stated purpose of the Final Report and Principles was to "guide industry in developing more meaningful and effective self-regulatory models."[14] The report expressed support for self-regulation "because it provides the necessary flexibility to address evolving online business models."[15]

Although the Final Report and Principles on behavioral advertising does not carry the force of law and is not even an official interpretation by the FTC or the FTC Staff of the FTC's Section 5 authority (prohibiting unfair and deceptive practices),[16] nonetheless they have served to stir activity and privacy-enhancing innovations in the behavioral advertising industry. The report was not just a pronouncement by the FTC of standards it felt appropriate for self-regulation, but a direct challenge to industry to live up to these principles.[17]

The implication was that the FTC was close to proposing or supporting legislation regulating the behavioral advertising industry or proceeding on its own with law enforcement actions. Indeed, the Final Report and Principles stated that "where appropriate [the FTC will] investigate possible unfair or deceptive acts or practices in violation of the FTC Act." It did just that with an enforcement action against Sears Holding Corp. in June 2009,[18] alleging that Sears Holding Corp. violated the FTC Act by failing to adequately disclose exactly what information an online tracking mechanism would collect from consumers.[19]

Principles for the Self-Regulation of Online Behavioral Advertising

Behavioral advertising is defined as follows in the Final Report and Principles:

> "[T]he tracking of a consumer's online activities ***over time*** – including the searches the consumer has conducted, the Web pages visited, and the content viewed – in order to deliver advertising targeted to the individual consumer's interests. ***This definition is not intended to include "first party" advertising, where no data is shared with third parties, or***

[13] http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

[14] *See* Final FTC Report and Principles at 11, *available at* http://www2.ftc.gov/os/2009/02/P085400behavadreport.pdf.

[15] *See* id.

[16] 15 USC Section 45(a) (making unlawful unfair methods of competition and unfair or deceptive acts and practices in commerce).

[17] Chairman Leibowitz (at the time a Commissioner) stated in his concurrence that "this could be the last clear chance to show that self-regulation can – and will – effectively protect consumers' privacy in a dynamic online marketplace." http://www.ftc.gov/os/2009/02/P085400behavadleibowitz.pdf

[18] http://www2.ftc.gov/opa/2009/06/sears.shtm

[19] Complaint and Final Decision and Order available *at* http://www2.ftc.gov/os/caselist/0823099/index.shtm.

contextual advertising, where an ad is based on a single visit to a Web page or single search query."[20]

The following four principles are set forth:

1. Transparency and Consumer Control – Enhanced Notice Outside of the Privacy Policy

This principle calls for a high notice and control standard, which the Commission considers to be consistent with existing consumer protection principles, which requires clear and conspicuous disclosures of material facts. In particular, every Website where data is collected for behavioral advertising should provide consumers with "a clear, concise, consumer-friendly, and prominent statement" that discloses the collection of data and gives consumers the ability to choose whether to have information about their clickstream behavior collected and used for these purposes.

While it is customary to provide notice and choice in a Website's privacy policy, the FTC encouraged companies to develop innovative methods of providing notice and control over data collection for behavioral advertising *outside* of the privacy policy. The FTC Staff also suggested that, in developing disclosure mechanisms, companies should look to empirical research as to what types of disclosures are effective.

2. Data Security and Data Retention for Information Collected Through Behavioral Advertising – Sliding Scale Used by FTC in Other Contexts

Companies are expected to provide reasonable security for data collected for behavioral advertising purposes, consistent with data security laws and FTC enforcement actions and guidance. The level of necessary protection may be flexible, on a sliding scale dependent on the data's sensitivity, the nature of a company's business, the risks faced, and the reasonable protections available. Additionally, the data should be retained only as long as necessary to fulfill a legitimate business or law enforcement need.[21]

3. Changes to Privacy Policies – Notice and Opt-In Consent for Material Changes Applied Retroactively

Companies should obtain affected consumers' affirmative express consent before using their previously collected data in a way that is materially different from the uses permitted under the privacy policy in place at the time when the data was collected. This principle requires a significant departure from current industry practices, which typically

[20] http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf at p. 46 (emphasis in original).
[21] Id. at pp. 37-39.

involve some form of robust notice, and may contain a time lag or an opt-out, or an ability for the user to quit the Website and have his or her data deleted.

4. Sensitive Data – Opt-In Consent for Use in Behavioral Advertising

Companies should obtain affirmative express consent before collecting sensitive data for behavioral advertising. There is little disagreement among regulators, industry, and advocates on this point, though there is significant and useful debate on what data should be considered "sensitive" and in what contexts opt-in should be required.[22] While the FTC Staff does not provide an exhaustive definition of "sensitive data," its report indicates that financial data, data about children, health information, precise geographic location information, and Social Security numbers would be considered sensitive.[23]

Further Steps By the FTC

In 2009 and 2010, the FTC conducted a broader exploration of privacy issues through a series of roundtable events bringing together over 200 representatives of industry, privacy advocates, academics, government agencies and other stakeholders and resulting in over 100 written comments. The outcome of this exercise is reported to be an FTC report on how privacy in general should be evaluated under the FTC's authority, taking modern technology and business practices into account. The report is expected in the fall of 2010, after which there will be a public comment period. Nevertheless, FTC Chairman Leibowitz has foreshadowed some of the issues that the FTC is considering in his recent Congressional testimony, and they continue to follow a cautious, balanced approach. For example, the FTC is considering a "just in time" notice as appropriate and more effective than standard privacy policies in some circumstances. Chairman Leibowitz also acknowledged that while some take issue with the specifics of how self-regulation is being developed in the United States, "many participants highlighted industry efforts to

---

[22] For example, a self-regulatory blueprint put forth by a coalition consisting of the Direct Marketing Association, the Interactive Advertising Bureau, the Association of National Advertisers, the American Association of Advertising Agencies, and the Council of Better Business Bureaus, released in July 2009, defines sensitive data to include data collected from children under 13, as well as financial account numbers, Social Security numbers, pharmaceutical prescriptions, or medical records about a specific individual. http://www.the-dma.org/government/ven-principles%2007-01-09%20FINAL.pdf

On the other hand, the Center for Democracy and Technology, in comments to the Network Advertising Initiative as it was developing its 2008 Code of Conduct, argued that the definition of "sensitive data" should be broader, including "information about past, present, or potential future health or medical conditions or treatments, including genetic, genomic, and family medical history information; information about an individual's sexual behavior, orientation, or identity (*e.g.*, lesbian/gay/bisexual/transgender); information about criminal victim status (*e.g.*, rape victim status); financial information; Social Security Numbers or any other government-issued identifiers; insurance plan numbers; and information that describes the precise geographic location of an individual."
http://www.cdt.org/privacy/20080612_NAI_comments.pdf

[23] Id. at p. 42.

improve transparency for consumers about the collection and use of their information." He also stated that one theme of the roundtables was the that regulators should be cautious in regulating the Internet:

> [C]ommenters and roundtable participants noted the tremendous benefits from the free flow of information. Consumers receive free content and services and businesses are able to innovate and develop new services through the acquisition, exchange and use of consumer information. Commenters and participants noted that regulators should be cautious about restricting such information exchange and use, as doing so risks depriving consumers of benefits of free content and services.[24]

B. Industry Response

In 2009, in response to the FTC's clear call to action, a diverse consortium of industry associations and nonprofit organizations came together to propose the framework for a self-regulatory program that will roll out in 2010. This group includes the Association of National Advertisers, the American Association of Advertising Agencies, the Direct Marketing Association, the Interactive Advertising Bureau, and the Council of Better Business Bureaus. This effort ("the Industry Self-Regulatory Response") is the most broad-based self-regulatory effort to date, as it brings together advertisers, advertising agencies, Web publishers, Internet access service providers, providers of desktop application software such as Web toolbars and Internet browsers, and online advertising networks.

The Seven Industry Self-Regulatory Principles

1. The Education Principle

Participants are obligated to take steps to educate consumers and businesses about online behavioral advertising. The industry has plans to do so through an educational Website and online advertising.

2. The Transparency Principle

A participant, whether a network advertiser site that use them, must employ multiple methods to clearly inform consumers about its behavioral advertising data collection and use practices. The goal is to move away from disclosure solely within the privacy policy, consistent with the FTC's stated concerns.

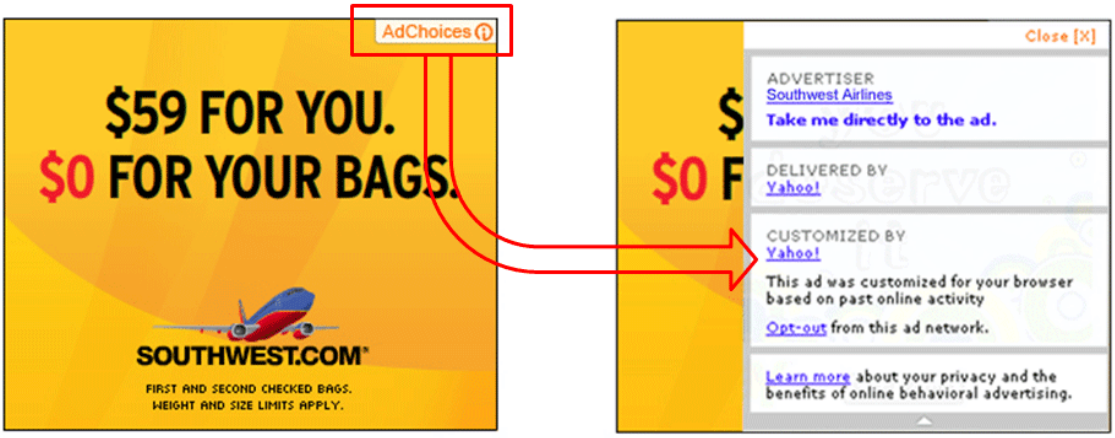
---

[24] Leibowitz testimony at 18-20.

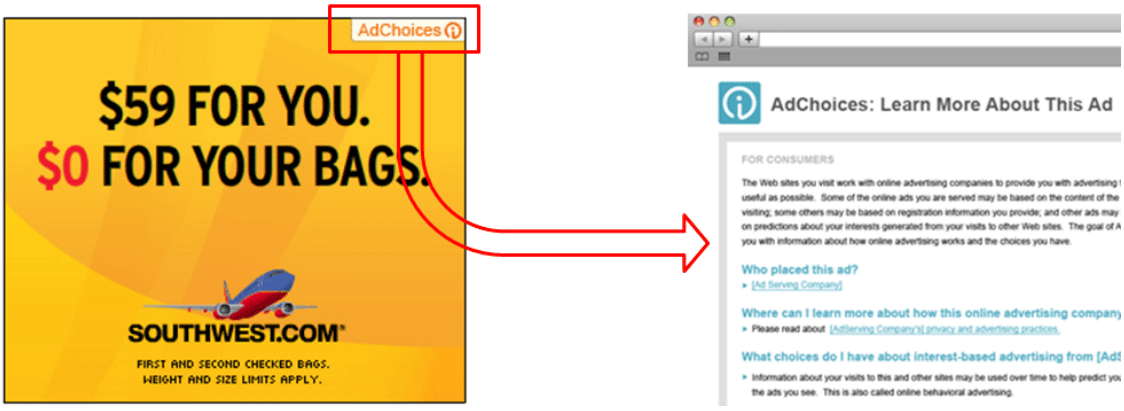
The result of this effort has been "the Power I" notice program, shown below in two examples released recently by the Direct Marketing Association and the Interactive Advertising Bureau. The essence of this program is an icon which indicates that an advertisement was behaviorally targeted; the icon leads to a landing page with information on how the advertisement was targeted and an opportunity to opt out.

Proposed Disclosure in Ads and After Consumers Click on Ads

- Example 1: Ad Marker opens an overlay Ad Interstitial populated with the Metadata



- Example 2: Ad Marker, using the Metadata, opens a new page (the Ad Interstitial) With information on the Ad and the Third Party



3. The Consumer Control Principle

Under this principle, visitors to Websites on which data is collected for behavioral advertising purposes must be able to choose whether their data is be collected, used and shared for such purposes. The choice mechanism will be provided by the entities that collect and use the data, either at those parties' own Websites or at industry-developed Websites. The new disclosures described above under the Transparency Principle will direct consumers to these mechanisms.

4. The Data Security Principle

Entities involved in the collection and use of information for behavioral advertising purposes must provide reasonable security for, and limited retention of, such data.

5. The Material Changes Principle

An entity must obtain the consent of affected consumers before it applies a material, less restrictive change to its behavioral advertising data collection and use policy to their data. Consent must be voluntary and free, but the Final Report and Principles does not use the word "express," allowing for a robust notice and opt-out regime for privacy policy changes.

6. The Sensitive Data Principle

An entity must comply with the Children's Online Privacy Protection Act with respect to information collected from or about children. In addition, consent is required prior to the collection of financial account numbers, Social Security numbers, pharmaceutical prescriptions, or medical records about a specific individual for online behavioral advertising purposes.

7. The Accountability Principle

This principle is one of the most important, as it seeks to establish a monitoring and enforcement mechanism, perhaps through the Council of Better Business Bureaus. The principles call for the online behavioral advertising industry to create and implement policies and programs that promote compliance with the principles.[25]

C. Assessment of the US Model

The FTC's prudential approach toward online behavioral advertising (*e.g.*, relying on strong guidance backed up by enforcement actions against those who flout that guidance) has been instrumental in fostering the development of a stronger regime in the United

[25] Both the Direct Marketing Association and the Council of Better Business Bureaus have indicated that they are either developing programs around the principles or integrating them into their existing programs.

States. The resulting industry proposed regime is inherently more flexible and enables organizations to adapt to new business models and new technological developments and deployments.

Targeted advertising benefits not only advertisers, but also large and small Websites alike. A recently released study[26] finds that targeted advertising, which by necessity requires tracking technologies such as cookies and Web beacons, supports online publishers in a substantial way. Specifically, the study found that:

a. The average CPM (cost per 1,000 impressions) for behaviorally targeted advertising is just over twice the average CPM for run-of-network advertising. On average across participating networks, the price of behaviorally targeted advertising in 2009 was 2.68 times the price of run-of-network advertising.

b. Advertising using behavioral targeting is more successful than standard run-of-network advertising, creating greater utility for consumers from more relevant advertisements and clear appeal for advertisers from increased ad conversion.

c. A majority of network advertising revenue is spent acquiring inventory from publishers, making behavioral targeting an important source of revenue for online content and services providers, as well as third party ad networks.[27]

This means that small publishers can grow, thrive, and compete with larger publishers because of their ability to attract larger fees for their advertising space. This, in turn, supports the continued development of the Internet's "long tail," and assures that the Internet will continue to thrive as a place where new ideas and new business models can incubate and ultimately flourish.

---

[26] The study was prepared by Professor Howard Beales, a Ph.D. in Economics and former Director of the FTC's Bureau of Consumer Protection.

[27] *See* Beales, The Value of Behavioral Advertising, *available at* http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf (March 24, 2010).

V. Conclusion

As the European Commission and Member States consider appropriate legislation for cookies, the GPA respectfully proposes that they consider the nuanced and flexible approach that is the result of decades of work in the United States and, that, in terms of cookies, is the most transparent yet.

Specifically, the GPA proposes that Member States consider a combination of enhanced notice and opt-out where necessary, and appropriate and certain instances of opt-in, narrowly tailored to protect consumers' privacy interests where they are most likely to be threatened. In this way, Member States would accomplish their duties under the e-Privacy Directive while giving European industry the opportunity to show the same kind of positive, privacy-enhancing innovation that industry has shown in the United States. This nuanced approach would preserve innovation and the sustained growth of the Internet, and all the many economic and cultural points of view that it is uniquely situated to encompass and provide.