

BEACONS, BUGS, AND PIXEL TAGS: DO YOU COMPLY WITH THE FTC BEHAVIORAL MARKETING PRINCIPLES AND FOREIGN LAW REQUIREMENTS?

By **Françoise Gilbert**

At the end of December 2007, the Federal Trade Commission (FTC) published a set of Proposed Principles to govern behavioral advertising (principles)¹ in order to create a framework for the collection of information through Web beacons and the use of this information when communicating with individuals or serving personalized advertisements. This practice is known as behavioral targeting.

Online behavioral advertising or behavioral marketing or behavioral targeting combines:

- Tracking online activities, such as searches that the user has conducted, Web pages that the user has visited, or content that the user has viewed. This is accomplished through the combined use of cookies and Web beacons, Web tags, clear GIFs, action tags, pixel tags, or Web bugs, and

- Delivering advertising targeted to a user's interests. Advertisements may be served to the user while he or she navigates the site. Personalized promotional emails may also be sent to that user with content focusing on the user's assumed interests.

Web beacons and other tracking technologies are not new. They have been in place for several years. What is new, is the substantial improvement in the precision and quality of the data collected and the use of this information for targeted advertisements.

The more accurate the data, the higher the risk of invasion of privacy. Since the early days of Web tracking technologies, industry groups and consumer advocates have developed proposals and recommendations regarding the issues raised by behavioral advertising. For example, a Do Not Track proposal was presented; it was inspired by the popular and highly successful Do Not Call program.

The principles recently published by the FTC encourage meaningful and enforceable self-regulation to address the privacy concerns raised by behavioral advertising. In its announcement of the principles, the FTC indicated that it intended to outline a framework to protect against harms to consumer privacy, while continuing to support innovation in consumer services and products.

The FTC stated that it remains mindful of the importance of accommodating the wide variety of business models that exist in this area. Concurrently, on the other hand, individuals must be protected against the risk that tracking technologies might lead to intrusion into their private affairs and the risk of abuse or misuse of sensitive personal information. Indeed, tracking mechanisms are largely invisible and unknown to consumers. Most consumers cannot see Web beacons and have no way to control them. They do not know whether they can block them or how to do so.

The issuance of the FTC principles also prompts a comparison with the equivalent regime in other countries. Indeed, companies with a global reach may need to understand more than just the principles outlined by the FTC. Since their Web sites or marketing campaigns may reach individuals protected by other laws, US companies must be prepared to comply with the laws of those foreign countries that may have jurisdiction over them.

European Union member states, for example, have issued rules or guidance on the use of Web beacons and tracking technologies in Web sites and email communications. While some common elements appear on both side of the Atlantic Ocean, there are additional twists and requirements in Europe, such as, notification of the Data

Françoise Gilbert is an attorney and a Certified Information Privacy Professional (CIPP). She is the Managing Director of IT Law Group, www.itlawgroup.com, a law firm based in Palo Alto, CA. Ms. Gilbert focuses on information privacy and security and data governance. She has assisted global companies and selected start-ups on leading-edge technology legal issues, including information privacy, information security, and other data governance issues. Copyright 2008, Françoise Gilbert.

Protection Authorities. This makes even more complex the operation of a Web site or the use of email marketing campaigns with a global reach.

This article presents an overview of Web tracking technologies, an analysis of the proposed FTC principles, and a survey of the laws applicable to Web beacons in selected European countries. A list of suggested best practices is also proposed.

WEB BEACONS

Web beacons, action tags, clear GIFs, Web tags, pixel tags, Web bugs, and similar tracking technologies are different from cookies. Web beacons are inconspicuous to the user. They consist of a small string of software code, typically 1-by-1 pixel in size, that is placed on a Webpage or an email message to track pages viewed or emails opened. Their size makes them invisible to the user. Their presence can be spotted only after scrutinizing the Web site code. They do not reside on the user's computer. Cookies, on the other hand, are easily identified on a user's computer. Go to the "Preferences" section of your browser.² Open the tab "Privacy," and then click on "Show cookies." A list of cookies is displayed.

Users can also set their browsers to accept or reject all cookies or only cookies from specified sites. Cookies can be deleted. In your browser's dashboard, click one of the two buttons under the list of cookies. You can delete all or only selected cookies. Thus, the user can keep some control over cookies. Not with Web beacons. Web beacons cannot be removed or deactivated by the user because they do not reside on the user's computer. Some sites, such as Yahoo, offer users the ability to click on an opt-out button, which blocks Web beacons placed by the company on its Web site.

Web beacons have been used for reporting site traffic, counting unique visitors, or to audit advertising. With the advent of technology, they are now also able to record almost every move of a Web site user, such as the areas of a page that the user has downloaded or printed or the ads on which the user has clicked. As a result, Web beacons are considered more invasive and are viewed as a greater threat to users' privacy than cookies.

Further, to the extent that they may also collect sensitive information about a user's lifestyle or concerns (such as frequent visits to specific pages of a medical site), there are substantial security implications. The data collected about the uses of a site may contain sensitive information, which may have to be guarded with substantial security measures.

HOW BEHAVIORAL MARKETING OCCURS

Behavioral marketing requires several components. In many cases, there is a combination of Web tracking technologies and cookie technologies. The user is identified through cookies. The use of the site is tracked through Web beacons. The collected data may or may not include personal information, such as the user's email.

Aggregate—non personally identifiable—data may be used to manage the site, identify the pages with greater traffic, or content that is viewed for a longer period.

If personal information has been collected, users may be recognized when they return to the site through cookies placed on their computers or through their computer IP addresses. In this case, the site (or a network advertising company) then may serve to the user advertisements that are based on the profile associated with that user's cookie. These personalized advertisements take into account the interest of the user, which were identified (or guessed) through the analysis of the prior visits of the user associated with that cookie.

In certain cases, contact information, such as the user's email address or user ID, may have been collected during other visits to the site or as part of the user registration process. In this case, in addition to serving advertisements, the company may combine the user's contact information and profile in order to create personalized promotional emails with proposals and promotions tailored to the user's interest. For example, the user who has shown interest for content or advertisements related to golf might be sent a promotion for a vacation in a golf resort.

BENEFITS AND RISKS OF BEHAVIORAL MARKETING

Behavioral marketing may offer substantial benefits to customers. For example, it may be instrumental in the provision of free Web content or access to newspapers and information, which are provided free because they are subsidized by online advertising.

In addition, behavioral marketing allows for the generation of personalized ads. The target customer might be more receptive to advertisements that are based on a personal profile. Someone interested in golf will likely be less annoyed by ads featuring Tiger Woods than by those that promote diet pills or cell phone services.

On the other hand, behavioral marketing is based on the use of data that have been collected without the user's knowledge because Web beacons are inconspicuous. The perspective of being monitored anywhere and everywhere on the Web makes Web surfing much less enjoyable.

PRINCIPLES PROPOSED BY THE FEDERAL TRADE COMMISSION

The FTC principles provide an attempt at funneling the tremendous development of behavioral marketing and limiting the possible attacks on customer privacy. The principles create a framework for the collection of information through Web beacons and the use of this information to serve targeted, personalized advertisements and other unsolicited communications to individuals. It aims at providing individuals with some control over their use of the Web. The principles are consistent with prior decisions made by the FTC in similar circumstances, such as in the *Gateway Learning* case.³

The proposed principles require:

- **Transparency.** A Web site where data is collected for behavioral advertising should provide a clear, concise, consumer-friendly, and prominent statement that data about consumers' activities online are being collected at the site for use in providing advertising about products and services tailored to individual consumers' interests.
- **Consumer control.** The statement should also provide that consumers can choose whether or not to have their information collected for such purpose. The Web site should also provide consumers with a clear, easy-to-use, and accessible method for exercising this option.
- **Reasonable security.** A company that collects and/or stores consumer data for behavioral advertising should provide reasonable security for that data. Such protections should be based on the sensitivity of the data, the nature of the company's business operations, the types of risks the company faces, and the reasonable protections available to the company.
- **Limited data retention.** The company should retain data only as long as is necessary to fulfill a legitimate business or law enforcement need.
- **Affirmative express consent for material changes to existing privacy promises.** A company must keep any promises that it makes with respect to how it will handle or protect consumer data, even if it decides to change its policies later. Therefore, before a company can use data in a manner materially different from promises the company made when it collected the data, it should obtain affirmative express consent from affected consumers.
- **Affirmative express consent to (or prohibition against) using sensitive data for behavioral advertising.** A company should only collect sensitive data for behavioral advertising if it obtains affirmative

express consent from the consumer to receive such advertising.

IN THE EUROPEAN UNION

The position of the European Union with respect to Web beacons, Web bugs, action tags, and clear GIFs includes some of the concepts outlined by the FTC, but differs in some aspects.⁴ For example, like for all other privacy protection matters, a company doing business in the European Union must "notify" its privacy practices to the Data Protection Authority of the country where it is located. Thus, the incorporation of Web beacons in a Web site that is directed to or sued by EU residents would require prior notification to the relevant Data Protection Authorities of the countries where a company does business.

In the European Union, Web beacons and other tracking technologies are largely considered equivalent to cookies, and their use in Web sites is generally permitted in European Union countries, subject to certain conditions. The specific rules in each country differ in their implementation, but generally require the following:

- The user must be informed of the use of these techniques and be given the option to refuse them, together with clear instructions on how to do so.
- If these techniques are going to be used to collect any personal data or data by which a user can be identified, the relevant Data Protection Authority must receive notification of the proposed use of tracking mechanisms by the site.
- The proposed use of the tracking technologies must be reflected in the site's privacy policy that is registered with the Authority.
- In some cases, the notification process will vary depending on the nature and criticality of the data collected.

When used in email or other direct communications, Web beacons, tags, and clear GIFs can be associated with a specific subject and are thus considered to collect personally identifiable information. As such, they are subject to the above requirements.

In addition, if these tracking technologies are used in connection with commercial emails (e.g., to track open rate), the recipient should be informed of their use and be provided with the ability to block them or switch them off.

There is currently no requirement for any special notification methodology to be used in order to notify users of changes in the privacy policy. In the United

States, the proposed principles published by the FTC would require companies to notify their users and obtain their opt-in consent to the new uses of their personal information, because the FTC views the use of tracking technologies associated with personal information as a “material change” from most prior practices.

UNITED KINGDOM

Although the current UK data protection legislation does not refer to web beacons, the guidance issued by the Information Commissioner Office’s (ICO) has been very clear about the use of web beacons or clear GIFs.⁵ The UK’s Privacy and Electronic Communication (EC Directive) Regulations 2003 implemented from EU Regulations (2002/58/EC) (the E-Privacy Directive) are the most relevant as these were drafted specifically with the increasing use of the cookie in mind.

The E-Privacy Directive introduced rules in relation to the use of cookies in 2003. The implementing UK regulations provide that cookies may be used only in the event that the user of the “terminal equipment” is provided with certain “clear and comprehensive” information about the purposes of the storage and access to the information gathered (whether or not such information is actually personal information). As with many privacy laws, the rhetoric of the law is to provide transparency to the user. To this end, as under the UK’s general data protection laws, the theory goes that, if users are provided with information about the purposes of such processing, they are able to make an informed choice as to whether they should accept it.

Linked to this, the rules state that users should be “given the opportunity to refuse the storage of or access to that information.” If they are offered the right to refuse such processing, the monitoring and tracking can be regarded as fair and lawful. This is effectively an opt-out system, and as such, users do not have to give their consent prior to the use of cookies.

The effect of these rules is that Web site owners have a specific obligation to alert visitors to the presence of *all* cookies and importantly give a choice as to their use. This is backed up by specific ICO guidance, which states that “at the very least, however, the user or subscriber should be given a clear choice as to whether or not they wish to allow a service provider to engage in the continued storage of information.” Guidance from the ICO goes on to confirm that, although not expressly referenced in current law, these rules would appear to affect all cookies, Web beacons, and pixel tags and not just those that involve the processing of personal data.

It should be noted that if personal data are also collected, the general rules of the Data Protection Act 1998 (DPA) would apply in addition. The DPA makes no specific reference to cookies or other technologies.

As the ICO has gone on record to equate Web beacons and clear GIFs with cookies, consequently the same cookie rules apply to these tracking technologies. A problem arises here. Although most browsers facilitate blocking or rejection of cookies, there are no similar tools available to reject or disable Web beacons, clear GIFs, or bugs (although disabling the cookie can frequently limit the ability to link certain personal information to that device).

As Web beacons and clear GIFs are frequently used in combination with cookies, they may result in the processing of personal data. Note that, in some circumstances, even an IP address can be personal data if it may identify a living individual. The ICO asserts that, when such devices are invisible, it is hard to see how the collection of personal data in this way can be “fair and lawful” and therefore in accordance with the DPA. The ICO suggests that users should be provided with information about the use of such devices and a technical means of refusing or disabling such devices.

However, as the Interactive Advertising Bureau of Europe (IAB) explains:

because web-beacons or clear gifs are the same as any other content request included in the recipe for a web page, frequently one cannot opt out or refuse them. One solution is to use them in conjunction with cookies, as they can then be rendered ineffective by either opting out of cookies or by changing browser settings.

Yet, even this is not necessarily enough. If the Web beacons are used to collect an IP address, for example, further care is needed as again the DPA regime applies.

Web beacons and clear GIFs can be used in marketing emails. In this regard, new ICO guidance states that when used in email communications:

The important point to note is that if you are using such a tracking device in your marketing emails, you must let the recipient know about it in the message itself and explain to them how to switch the web beacon or clear gif off. You could provide this information next to your valid address for opt-out requests and include a link to a webpage that offers a fuller explanation. A link to your cookie and privacy policy alone is unlikely to be sufficient unless the section of that policy which relates to the use of web beacons or clear gifs is clearly signposted when you arrive at that page.

FRANCE

There is no legislation specifically addressing the use of Web Beacons, but if the data collected will be used for targeted marketing messages, they are subject to the French Data Protection Law and to the law of June 21, 2004, Trust in the Digital Economy. To the extent that the beacon records such information as the number of pages viewed, which sections were viewed, and the time spent on each, the French Data Protection Law requires that:

- The user must be informed of the use of the beacon and the purpose of the data collected.
- The user must have the option to reject the data collection.
- The user must be given appropriate instruction to exercise his/her opt-out right.
- Notification must be given to the CNIL (French Data Protection Authority) advising them of the use of these techniques and explaining what has been implemented to inform the users and advise them of their rights.

It is permissible to include the user notifications in the originating site's privacy policy.

If the information collected is used to drive marketing messages sent electronically to the customers or prospects, the Trust in the Digital Economy law also requires prior consent from the user.

In addition, the law of July 10, 1991, about the protection of the secrecy of correspondence (paper and electronic) protects the content of emails as private correspondence. Thus, to the extent that a Web beacon would be used in emails, it might infringe upon the secrecy of the correspondence. For example, if a Web beacon is used to read the content of the email, it would be disclosing information about the correspondence that might be infringing on this law.⁶

GERMANY

Web beacons are likely to be seen as comparable to cookies as their intention is to provide the person installing the Web beacon a means of gathering information on the user. This information is then used to generate user profiles (in most cases for marketing purposes). If the data collected by the Web beacon includes "personal data" as defined by German Data Protection Law, it is subject to the relevant provisions of either the Federal Data Protection Law or the Tele Media Law (which replaced the Teleservice Data Protection Law with effect on 03/01/2007).

Since most Internet users do not have static IP addresses, but dynamic IP addresses, in Germany Web beacons on Web sites are able to collect personal data only if they are combined with Web site cookies that collect personal data. Otherwise, it is unlikely that the user is identifiable. This would be different with regard to Web bugs used in emails and if the Internet user has a static IP address and therefore is identifiable for the person installing the Web beacon.

In general, under both the Federal Data Protection Law and the Tele Media Law, the collection, processing, or use of personal data is justified only if permitted by law or if the person whose personal data is to be collected, processed, or used has given his/her consent in advance. Therefore, if the personal data collected by the Web beacon is not necessary to provide the service (which would constitute a legal permission under the Tele Media Law), the collection is subject to prior consent.

Furthermore, certain obligations to inform the Internet user email/recipient apply if the Web beacon contained therein is to collect personal data. It is likely that a disclaimer that only states that the Web site uses Web bugs/Web beacons would not be sufficient since the data subject has to be clearly informed about the type of personal data collected and the purpose of collection, processing, and use. In the event the web beacon is not contained in the Web site visited but in a Web banner the ad-server provider would be subject to the information obligation.

Even when the Web beacon is used to create an anonymized user profile, the user has to be informed that he has a right to object to the use of the Web beacons.⁷

ITALY

There are no specific provisions covering Web beacons or the like in Italy. However, since the Italian Law of 1996 has adopted the 2002 Directive, the situation there is largely consistent with the rest of Europe in that the data subject must be informed as to the use of his data and the related purpose. If the data collection is not necessary to provide the service to the user, user consent will be necessary.

Both the Italian consumer protection laws and the Italian Data Protection Law state that any marketing activities that involve the use of the Internet, MMS, or SMS require the prior consent of the data subject. In addition, any processing of personal data whose purpose is to profile consumers or data subjects in general is subject to prior notification to the Data Authority. Notification is merely a form of communication to the Data Protection Authority and no approval is required after notification.

It has to be pointed out that the Italian Data Authority has recently tightened its requirements on the use of Internet or email addresses to send promotional, commercial, or marketing materials in general. Thus, the principle applied is that any electronic communication to a customer or prospect requires prior consent of the data subject.⁸

SPAIN

According to Spanish regulations on data protection, Web beacons are allowed as long as they collect only information that includes neither personal data nor data by which the user can be personally identified. Web beacons can be used freely as long as they are used only to control the effectiveness of an advertising campaign or similarly by collecting data such as information which has been assigned to a specific cookie, such as the time and date when a Web page has been viewed and a description of the Web page where the Web beacon is residing.

If, however, Web beacons or cookies are used to collect personal data, they are subject to prior notification to the Spanish Data Protection Authority. The corresponding privacy policy must be registered with the Data Protection Authority through the notification process.

The notification to the Data Protection Authority must specify that these tools will be used as a means to collect personal data. In such case, notification proceedings may differ depending on the type of data that is collected, requiring a high, medium, or basic level of protection, according to Law 15/1999 on Personal Data Protection.

Further, when the Web beacons or cookies are used to collect personal information, this must be pointed out in the terms of use or privacy policy of the Web site.

The user must be given the possibility of accepting or rejecting the use of the electronic tools (Web beacons, cookies, etc) by being offered the relevant tools and instructions to do so.

These specifications also apply to third-party Web beacons.⁹

IP ADDRESSES AS PERSONAL INFORMATION IN THE EU

Companies doing business in the European Union should also remember that IP addresses are considered “personal information” in the European Union. For example, Peter Scharr, the Germany Data Protection Commissioner, who leads the EU group preparing a report on how well the privacy policies of Internet search

engines comply with EU privacy law, recently stated at a European Parliament hearing on online data protection that when someone is identified by an IP, or Internet protocol, address, “then it has to be regarded as personal data.” While this concept had been advanced numerous times in Europe among data privacy professionals, there is now a confirmation that IP addresses should generally be regarded as personal information.

This statement might affect companies that use Web beacons and collect IP addresses. Indeed, if an IP address is deemed “personal data,” then using tracking technologies in connection with IP addresses might constitute the collection of personal data protected under the European Data Protection laws. This might make most uses of Web beacons subject to the notification requirements outlined above.

SUGGESTED MEASURES FOR US BASED COMPANIES

While the FTC principles are not final and are open for comments, they provide a clear indication of the FTC’s position with respect to the use of tracking technologies and what rules might be used in the near future to evaluate the adequacy of tracking technology usage. In the past, the FTC has proactively used its powers under § 5 of the FTC Act to prosecute companies for their data protection practices. It is likely that it will continue to do so, and that policing the use of tracking technologies will remain among its priorities.

Companies contemplating the use of tracking technologies should assess their impact on the privacy rights of their Web site users and the types of disclosures and consent that might be needed before proceeding. To the extent possible, companies should follow the course of action provided in the principles in order to be prepared if these proposed terms became final.

Until the principles are finalized and formally adopted, US companies that are using or intend to use tracking technologies on their US Web sites other than as clearly described in their current Web site privacy statements should consider the following:

- **Assessment:** Investigate the scope of the use of these technologies, the types of information that they collect, and the types of cookies with which they are associated. Look at both your practices and those of the advertising networks that you use to serve advertisements on your site and on third-party sites.
- **Notice:** Inform users about the use of tracking technologies, what information will be collected, how it will be used, for which purpose, and to whom the

information will be disclosed. Provide the notice in clear and conspicuous language before the user's information is collected.

- **Information:** Inform users that the company's policies have changed. In some cases, opt-in consent to the use of the new technologies with personal information that the company may have collected in the past may be necessary because there might be a material change from the prior practices.
- **Choice:** Inform users about the choices and means that your company offers for limiting the collection of information through Web beacons; offer users the opportunity to choose whether their information may be collected. Provide users with the means to block the use of tracking technologies when they are or might be associated with the collection of personal information. Provide a clear, conspicuous, and readily available mechanism to exercise this choice.
- **Sensitive information:** Do not collect sensitive information of individuals without their affirmative or explicit consent. The proposed principles provide for opt-in consent.
- **Limited Use:** Limit the use of the information collected through tracking technologies to the purposes identified in the disclosures. Keep the data only for the time necessary to achieve the purposes stated in your policy. The principles provide that data should be retained only as necessary to fulfill a legitimate business need.
- **Security:** Take reasonable precaution to protect information collected through tracking technologies against loss, misuse, unauthorized access, disclosure, or alteration as appropriate, given the potential sensitivity of the information.
- **Emails:** If tracking technologies are used in email communications (e.g., to track open rate), consider, as well, appropriate notification and information on how to block the beacons.
- **Notification:** If the company is also doing business in the European Union, file the modified privacy statement with the relevant Data Protection Authorities in the countries where it does business in order to comply with the notification requirements that are in place in each of the EU member states.

Since the use of tracking technologies and the collected information is likely to constitute a change from prior practices, ensure that the users are made aware of the change to prior practices. The principles clearly indicate that the FTC believes that the use of tracking technology constitutes a material change to most companies'

practices. Consistent with its prior rulings, the FTC suggests that the materiality of the change requires that you obtain affirmative express consent to the new use of visitors and members' information, especially when the information that will be collected through the use of the tracking technologies might be combined with personal information that the company has collected in the past under a different privacy policy that did not provide for the use of tracking technologies.

To do so, at a minimum, conspicuously post a notice of the upcoming changes to the privacy policy on the Web site. Ensure that users have a reasonable time to become aware of the change before the launch. Provide users with the means to choose not to have their use of your Web site tracked through web beacons.

CONCLUSION

Pixel tags, Web beacons, and clear GIFs have existed for several years. Initially used for counting the open rate of emails or computing advertisement fees, they are becoming ubiquitous on Web sites and the use of the data collected is expanding drastically. This is because recent improvements to the technology allow the collection of data that are more granular, more precise, and of higher quality. With better data, advertisers can identify with greater certainty the interest, preferences, and needs of those who use or visit their Web sites. By applying these more refined data to the creation of personalized messages, companies hope to provide their target customers with more meaningful or useful messages and increase the efficiency and return on investment of their marketing campaigns.

The increased data quality allows the compilation of information about a user's interests that is likely to be more accurate. If the collection of personal data about an individual can occur regularly without the individual's knowledge or consent, the privacy, and potentially the security, of that individual may be at risk. The proposed FTC principles present a set of best practices that are consistent with fair information practices. While the document is only a first draft for which comments have been requested, it nevertheless constitutes the best pictures of the current position of the FTC with respect to behavioral targeting.

Companies that want to be privacy leaders should promptly implement clear and conspicuous policies that are consistent with the proposed FTC principles and give users of their website the right and ability to consent to the use of these technologies to collect personal information, or the tools necessary to block these technologies.

NOTES

- 1 <http://www.ftc.gov/opa/2007/12/principles.shtm>.
- 2 The Firefox browser is used in this example.
- 3 <http://www.ftc.gov/opa/2004/07/gateway.shtm>.
- 4 The author thanks Alain Bensoussan (Alain Bensoussan Avocats, Paris, France); Axel Funk (CMS Hasche Sigle, Stuttgart, Germany); Gerald Graefe (CMS Hasche Sigle, Stuttgart, Germany); Carlos Millan (Batalla Abogados, Madrid, Spain); Mark Webber (Osborne Clarke, Reading, England); and Raffaele Zallone (Studio Zallone, Milan, Italy) for their contributions and comments to this section.
- 5 The information in this section was graciously provided by Mark Webber.
- 6 The information in this section was graciously provided by Alain Bensoussan.
- 7 The information in this section was graciously provided by Axel Funk and Gerald Graefe.
- 8 The information in this section was graciously provided by Raffaele Zallone.
- 9 The information in this paragraph was graciously provided by Carlos Millan.