Web Tracking and Privacy

Three questions to ask your marketing automation provider

11/15/2010

ClickDimensions – Email Marketing and Marketing Automation for Microsoft Dynamics CRM

Web Tracking and Privacy

Three questions to ask your marketing automation provider

The subject of this writing was inspired by a call with a prospective client who asked if the web tracking component of the ClickDimensions marketing automation product could identify a visitor who had never revealed himself to their web site. By 'reveal' we are referring to the completion of a web form or a click on a link from an email that was sent by the site. Either of these actions is a way for a site to know, within reason, the identity (i.e. email address) of the visitor. To answer the prospect's question required an overview of available web tracking methods and their implications on visitor permissions and privacy. At the end of the conversation, the prospect was aware that while it is technically possible to provide the capability they requested, doing so involves sharing visitor data. Needless to say, the prospect withdrew the request. They are now a happy ClickDimensions customer with full knowledge of how our tracking technology works and an updated privacy policy making their visitors aware of how our technology is used on their site.

It is our belief that companies that wish to employ web tracking technology responsibly must know how their provider is doing it on their behalf so they can confidently disclose these methods to visitors in their privacy policy. The method you select has the potential to shape not only your short and medium term web marketing results, but the very image of your business in the marketplace.

If you are considering a marketing automation provider to help meet your goals, consider asking them the following questions:

1. **"What are the rules and best practices regarding permission and privacy?"**
   And will your marketing automation provider follow them?

   With respect to email marketing, which has been in the mainstream much longer than web tracking, responsible marketing automation providers will not hesitate to advise their prospective clients to:

   - Obtain permission before adding someone to an email list, and
   - Make it easy for recipients of emails to unsubscribe

   It is widely accepted that, without explicit consent of subscribers, companies should not share their email addresses with third parties. Further, we know that mailing to purchased lists of people who have not requested our mailings is breaking the rules.

   When these rules are broken, most of us are not happy and the internet service providers who control whether our emails get delivered begin to block such e-mail traffic.

   In short, permission marketing is now the standard and there are consequences for those who ignore it or are unaware they are out-of-bounds. Be sure that your marketing automation provider acknowledges and follows accepted best practices regarding permission and privacy to ensure your business attracts and retains customers, rather than repels them.

2. **"What tracking methods do you use?"**
If the marketing automation provider does not want to disclose this, then why not?

Buyers of marketing automation solutions like ours are intrigued that they can learn about visitors on their sites and the actions those visitors take. However, not all of us are educated as to how that tracking actually occurs. If we want the information badly enough, we and our providers could take a "don't ask, don't tell" position. However, if we believe in individuals' right to privacy, then we can't make this argument. Let's take the mystery out of web tracking so you can ask important questions to marketing automation providers and decide for yourself and your business what is acceptable and what is not. Remember that, regardless of which tracking methods you endorse, you should be clear with your visitors (in a published privacy policy) as to how they are being tracked and how their information is being used.

To fully understand the impact on customer receptivity to web tracking methods, consider the mechanics of web tracking as if *you* were your own web visitor:

Background. We'll begin with a very basic premise. The modern browser is not engineered to give away your personal information. Barring a bug, hack or hole, companies like Microsoft, Google, Apple and Mozilla are not in business to tell web sites who you are. So, to determine who you are, tracking technologies need some method of creating a link between you and your browser (or your computer). This link is typically what is referred to as a cookie. A cookie is traditionally a text/HTML file that is placed in your browser and includes a unique identifier that is meaningful only to the site that placed it. With each visit you make to that web site, the site can look for the cookie and check its identifier against the web site's database to see if you have visited before.

Site-Specific Tracking

If, during one of your visits, you tell the web site who you are by completing a form or clicking on a link in an email sent from the site, then the unique identifier in the cookie can be associated with your personal information (i.e. your email address) so that each time you return to the site, you will be recognized. We'll refer to this type of tracking as site-specific because the site you are visiting has determined who you are through only your interactions with their site, and without help from other sites. In order for site-specific tracking to be responsibly employed, organizations using it should practice a permission-based email marketing policy so that visitors identified through email link clicks must have signed up for those emails on the site or otherwise given their explicit consent to receive them.

Multi-Site Tracking with Universally Unique Identifiers (UUID)

An alternative method of tracking is through the use of cookies containing universally unique identifiers (UUID) that are shared across multiple sites. In some cases, advertising solutions place cookies on your computer so that ads served to you on

various web sites can be tailored to your specific demographics and interests. There are two ways that cookies can accomplish this. Either the cookie can contain anonymous information indicating the visitor's demographics and interests (e.g. information that indicates only that the visitor is male, 35 – 55 years old and a sports fan) or the cookie can contain personally identifiable information (PII) such that the site can know the exact identity of the visitor. The latter is accomplished by placing a universally unique identifier (UUID) in the cookie so that other sites can read that identifier and reference a shared database that tells the site exactly who the visitor is, along with all the information that it and the collaborating sites have collected about the visitor. So, if you visit site A and identify yourself by providing personal information and then site A shares that information with site B, then site B can know who you are even though you haven't identified yourself to site B. Multi-site tracking can be enriching for the user when it does not involve personally identifiable information (PII) such as what is available through the use of universally unique identifiers (UUID). However, to visit a site, share with it your personal information and then have it share that personal information with other sites is an invasion of privacy unless you are aware it is happening, agree to it, know exactly what information it is sharing about you and to which sites your information is being shared.

3. **"Do your web tracking methods employ Adobe's Flash player?"**
Avoid violating Adobe's policy and misleading visitors to believe they are not being tracked when they are

Web browsers may be set to accept or block cookies, as well as retain them or delete them. So, if we don't want to be tracked, deleting and/or disabling cookies will avoid it, right? Not necessarily. It is possible to store information outside of the browser so that the normal process of cookie deletion will not rid your computer of the identifying information.

This is commonly done by storing identifying information in your computer's Flash player preferences area. Since Flash was designed with a common preferences area for settings like 'Volume' and 'VolumeMuted' (this common area is called 'local shared objects'), marketers quickly realized that they could use this area to store their identifying information so it wouldn't be removed in the normal cookie deletion process (or so it could re-populate a cookie that a user deleted specifically to avoid tracking). This approach seemed too good to be true because, since most computers have Flash installed, and Flash is unique to the computer and not the browser, storing information in the Flash preferences area allowed them to identify the visitor even if he or she used multiple browsers on the same computer and routinely deleted their browser cookies. Some vendors take their use of Flash cookies to an even more disturbing level by using them re-create normal browser cookies even after you delete them. This is a practice referred to as re-spawning.

Is this acceptable? Well, for starters, the Adobe terms of service prohibit Flash being used in this manner. Further, consider how you will write a privacy policy for your site explaining that

you are violating the Flash terms of service for the sole purpose of tracking your visitors - even when they have taken the right measures not to be tracked. This is not exactly a permission-based practice so it is no coincidence that top marketing automation vendors like Eloqua, Marketo, Pardot and, of course, ClickDimensions, do not use flash cookies in their products. The resources section at the end of this document provides links to some articles on this controversial technique including an article titled why Flash cookies should be banned for advertising.

Our position

So, what is right and what is wrong? Well, we've all seen this movie before and we know how it will end. Permission and transparency will rule. This doesn't mean tracking will come to an end. To the contrary, those that do it well and disclose how they do it will gain their visitors' trust, provide them value, enrich their experience and serve them better. However, those that choose to track us in ways that we do not understand and cannot control will simply make us angry and drive us away.

Only practices that respect consumer privacy and permissions can establish the trust businesses must seek to ensure positive initial *and repeat* customer experiences, as well as increase the likelihood of referred business. ClickDimensions is passionate about helping shape the respectability and consumer perception (and reception) of responsibly-employed web tracking technology. We want prospective clients to be informed and make good decisions without regard to whether they ultimately engage ClickDimensions to partner with them to meet their goals. It is in that spirit that we provide informational tools like this article.

Of course, we invite opportunities to answer your questions, and the privilege of being considered as your provider of marketing automation solutions. As you might expect, we believe that, as a provider of tracking technology, we and our customers are obligated to publish a clear privacy policy outlining the technologies we use for tracking and our use of the information we track. Our policy can be seen at http://www.clickdimensions.com/privacy and it clearly outlines what we are doing and how we do it.

Resources:

- Cookies 101: https://www.rapleaf.com/people/cookies101
- Code That Tracks Users' Browsing Prompts Lawsuits: http://www.nytimes.com/2010/09/21/technology/21cookie.html
- Why Flash Cookies Should Be Banned for Advertising: http://blog.rapleaf.com/why-Flash-cookies-should-be-banned-for-advertising/
- Adobe Flash Player Storage Settings panel (Adobe's web page that shows you what is stored in Flash cookies on your computer) http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager07.html
- Actual location of 'flash cookies' on computers running Microsoft Windows C:\Users***yourusername***\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\

Note: when inspecting the flash shared object directory on your computer be aware that many entries are there for the intended use of that area and contain Flash related settings (e.g. Volume, VolumeMuted, etc.). Others are there solely for tracking.

Contact:

For more information or questions regarding ClickDimension's stance on privacy issues please email privacy@clickdimensions.com