The Effect of Behavioral Targeting on Trust in E-Commerce

By Catherine Dwyer
Pace University
cdwyer@pace.edu

Abstract:

Behavioral targeting is an online marketing method that collects data on the browsing activities of consumers, in order to 'target' more relevant online advertising. It places digital tags in the browsers of web site visitors, using these tags to track and aggregate consumer behavior. Most data is collected anonymously, i.e., not linked to a person's name. However, behavioral targeting does create digital dossiers on consumers that connect browsing activity to a tagged individual. This tagging is largely invisible to consumers, who are not asked to explicitly give consent for this practice. While this is presented as beneficial because it delivers a more personalized e-commerce experience, this paper will argue that behavioral targeting in its current form is damaging to trust in e-commerce. To document this damage, Whitworth's polite software framework will be applied to three case studies of behavioral targeting. Whitworth argues politeness is an important social requirement of software, defining politeness as "offering the locus of control of a social interaction to another party." This paper will show that behavioral targeting is impolite, and by using data collected clandestinely it undermines the autonomy of consumers in their online shopping and purchase decisions, thus eroding trust in e-commerce.

Keywords:

Behavioral targeting, Trust, Electronic Commerce privacy, Clickstream tracking, Social Impacts, Socio-technical Design

Introduction:

Trust is an important ingredient of e-commerce, and lack of trust leads to lost customers and business opportunities (Gefen, Karahanna, & Straub, 2003, p. 19). Trust is defined as the willingness of

one party to be vulnerable to the risks of misbehavior by another party (Benbasat, Gefen, & Pavlou, 2008). It depends on confidence and faith rather than explicit control in an ongoing relationship (Fukuyama, 1995). The willingness to enter a relationship requires trust in the opposing partner's respect for privacy. Trust and privacy have a complex, but mutually dependent relationship. Trust can influence privacy management, and privacy breaches can damage trust (Petronio, 2002).

The issues of privacy and trust are central when considering behavioral targeting and e-commerce. Behavioral targeting refers to a group of technologies that gather information about a consumer's online activities in order to deliver advertising targeted to potential upcoming purchases. By observing the Web activities of millions of consumers, the aim is to closely match advertising to potential customers. Data collected includes what web sites you visit, how long you stay there, what pages you view, and where you go next. This data collection is described as anonymous because it does not collect information such as your name, address, email address, phone number and so forth. However, the primary activity of behavioral targeting is to continually try to tag consumers with a unique identifier used to aggregate their web activity over time. This collection of data used to influence an anonymous but uniquely identified consumer has triggered a public debate about the impact of these practices on consumer privacy (Clifford, 2009; Cohen, 2009; Story, 2007).

Behavioral targeting is quite widespread, and is a dominant method of implementing online advertising (FTC, 2009). It is therefore important to consider what effects the practices of behavioral targeting may have on trust in e-commerce. Trust is critical for a functioning commercial market, either online or offline. A functioning market relies on common social understandings of roles, obligations, and rules for exchange (Mankiw, 2000). These social understandings form expectations and norms that influence the relationship between buyer and seller. Norms curb opportunistic behavior that undermine the viability of economic exchanges (Platteau, 1994). Frequently these norms are codified into industry self-regulation or government regulation, but informal norms and expectations can play a powerful role in "sustaining honest behavior" (Platteau, 1994, p. 753).

The general social expectations of the market are as follows. Sellers expect buyers will pay a fair price for goods, and will not engage in fraud. Buyers expect that sellers will not employ deceptive practices by hiding information relevant to the transaction, or break promises (Platteau, 1994). These expectations form a social contract that encourages the smooth operation of market transactions. The etiquette of the marketplace is a social shorthand, a signal if you will, that allows one to quickly infer the intent of another party (Miller, 2004). The control of fraud and deceit are the most common regulating mechanisms found in commercial markets (Platteau, 1994).

A market that offers no control over fraud or deceit can be less efficient from an economic point of view because each commercial actor must vet the intentions of their trading partner (Williamson, 1985). This can be quite time consuming and expensive. Instead, if a market successfully signals the regulation of fraud and deception, the default condition between new trading partners will be trust. A functioning market assures that, in the absence of evidence to the contrary, buyers and sellers will trust partners in economic exchanges (Platteau, 1994).

Firms that successfully meet the social expectations of customers will be more competitive. The management of customer expectations has been the focus of training for both sales staff (F. R. Dwyer, Schurr, & Oh, 1987) as well as customer service representatives (Kelley, 1992). Since customers have social expectations when they engage in commercial activity, what are their social expectations of an e-commerce site? The discussion of social expectations of e-commerce has largely focused on the issue of trust (Alpert, Karat, Karat, Brodie, & Vergo, 2003; Benbasat et al., 2008; Metzger, 2004; Tang, Hu, & Smith, 2008; Turel, Yuan, & Connelly, 2008).

One complexity of this research is that trust has been defined as an interpersonal construct. Since the computer is a machine, the discussion of trust and e-commerce becomes anthropomorphic (Benbasat et al., 2008). The problem of anthropomorphism relates to firstly, interpreting the social expectations of

customers towards an e-commerce site, and secondly, setting design requirements for how an e-commerce site should "behave."

With regard to the first issue, studies show people do indeed treat computers as "social actors," and do not consider their social reactions as problematic in any way (Nass, 2004; Nass, Steuer, & Tauber, 1994). The second issue requires a definition of the social expectations users have of computers. Do users expect technology to conform to the norms of market exchanges? Do people have ethical and social expectations for the actions of computing systems, and how do they respond when their expectations are not met?

One way to determine whether a site matches the social expectations of commercial transactions is suggested by Miller (2004), who recommends asking these two questions:

1) If this system were replaced by an ideal human assistant, albeit one constrained to act through the interface modalities available to the system, how would that assistant behave?
2) If a human assistant were to provide this interaction in this way, how would he or she be perceived by colleagues?

An example of a method that seeks to design systems in line with social expectations is value based design (Flanagan, Howe, & Nissenbaum, 2008). The goal of value based design is that "the agents of an enterprise reflect the appropriate values in their interactions with users …[It is] the practice of designing with values in mind … [and] for systematically bringing values into the process of design," (Flanagan et al., 2008, p. 323).

Another method that evaluates the social effect of software is the work of Whitworth, who presents a framework for polite software (Whitworth, 2005, 2009). In the next section, Whitworth's description of polite software will be presented, and then applied as a framework with which to analyze behavioral targeting, and its impact on trust.

The Polite Software Framework

Whitworth argues that "politeness" makes society "a nicer place to be," and performs an important function in civil society by promoting cooperative versus competitive behavior (Whitworth, 2005, 2009). When we are all selfish, as in the tragedy of the commons, then society suffers. Selfish software, by comparison, takes over your computer for its own purposes, installs itself and begins automatically at startup, and in general dominates your interactions with your computer, including setting default values that reflect its own interests. In many ways online social spaces have been invaded by selfish software that degrades the nature of the online experience.

To apply politeness to software it must be defined "in information terms, as offering the locus of control of a social interaction to another party," (Whitworth, 2005, p. 353). Politeness is an extension of HCI, making it as a social requirement for interactive software. It moves interactions from competition to cooperation, creating win-win social synergies that lead to more prosperity, and moves away from conflict. For more on the analysis of polite software see (Whitworth, 2005, 2009).

Whitworth emphasizes that it is critical to understand that politeness goes beyond what is legal, beyond the standards set by the law. If you stop at a red light, that is not polite because you are expected to do so. Politeness, by exceeding what is merely required, can offer social flexibility. "Laws cannot cover every case. Without politeness, rules could multiply like weeds, creating a legal system that is expensive for society to run," (Whitworth, 2005, p. 355).

Politeness is relevant to defining the social expectations of market actors. A critical characteristic of effective sales staff is politeness and respect for the customer (F. R. Dwyer et al., 1987; Kelley, 1992). Politeness communicates a key requirement of the market, which is signaling recognition of the autonomy of the consumer. In a similar vein, the politeness of the consumer towards the seller signals recognition of the economic value the seller provides in an exchange.

Whitworth describes four rules with which to evaluate the politeness of software, which are the following (Whitworth, 2005, pp. 358-359):

Rule 1: Polite software respects, and does no preempt, rightful user choices.

Rule 2: Polite software declares itself and its social source.

Rule 3: Polite software helps users make desired choices.

Rule 4: Polite software remembers past user choices.

Rule 1 addresses the dynamics of human computer interaction. If a resource is to be consumed, or set of possible actions to be selected, then polite software would offer choice to the user, and especially not impose choices that serve the software's interests over those of the user. Rule 2 relates to a requirement that all software clearly identifies the social actor they represent, such as a behavioral targeting or advertising network. Rule 3 relates to the usability of software help that guides the user in understanding choices available, and the consequences of those choices. Rule 4 says that polite software remembers a user's preference or past settings, and applies those preferences when determining choices in new interactions.

The next sections will apply the polite software framework to behavioral targeting. First, a brief overview of behavioral targeting practices will be presented. This will be followed by three case studies of behavioral targeting. Each case will be evaluated using the polite software framework to capture the social reasons why behavioral targeting is damaging to e-commerce. Because consumer objections to behavioral targeting are emotional and hard to articulate, marketers often dismiss them as hysteria or overreaction. By understanding how exactly behavioral targeting is impolite, the result is a stronger argument for why it is harmful to e-commerce.

An overview of behavioral targeting

Behavioral targeting involves the collection of information about a consumer's online activities in order to deliver advertising targeted to their potential upcoming purchases. For example, say a consumer from Washington, DC shops online for airline tickets to New York City. She searches for flights, but doesn't make any purchases yet. She subsequently visits the web site of the local newspaper, where she sees a targeted ad offering flights between Washington, DC and New York City. While the consumer has not been identified by name, her interest in airline tickets has been noted, both by placing a cookie on her computer, and collecting and logging her airline shopping behavior (FTC, 2000).

Behavioral targeting is conducted by companies generically identified as advertising networks. By observing the Web activities of millions of consumers, advertising networks can closely match advertising to potential customers. Data collected includes what web sites you visit, how long you stay there, what pages you view, and where you go next. The typical data gathered does not include your name, address, email address, phone number and so forth. In this sense, the data collected is 'anonymous.' However, the clear intent of behavioral targeting is to track consumers over time, to build up digital dossiers of their interests and shopping activities. Even though names are not collected, these companies do continually try to tag consumers with a unique identifier used to aggregate their web activity. The most well known method for tagging consumers is with cookies, although methods such as Web beacons and Flash cookies are actively used.

Description of Behavioral Targeting Technology

Behavioral targeting is a generic name for a series of technologies that collect and organize click stream data, develop data warehousing structures, apply data mining algorithms to uncover consumer browsing patterns, and serve targeted ads matched to an individual. Behavioral targeting customizes messages to individual consumers based on their specific shopping interests, and characteristics such as gender, age, and ethnicity.

Advertising networks increase their ability to collect data by establishing relationships with partner Web sites. Examples of partner Web sites include news, entertainment, media, gaming, and blogging sites. Some of the largest advertising networks include Advertising.com, Inc., Akami Technologies, Blue Lithium, TACODA, 24/7 Real Media, Tribal Fusion, DoubleClick, and Atlas Solutions (NAI, 2009).

Behavioral targeting embeds a tag or identifier within a consumer's browser, using that tag to track browsing behavior. This digital tag does not identify a consumer by name. It functions more like an internal code or index that can connect non-contiguous browsing sessions.

Behavioral targeting divides browsing information into 'personally identifiable information' (PII) and not personally identifiable (non-PII). Categories of PII include name, email address, and social security number. Non-PII is basically everything else about you, including your age, gender, ethnicity, what sites you visit, and what pages you view. The collection of non-PII is carried out by many e-commerce sites without explicit consent from consumers. It is the use of behavioral targeting to collect non-PII that is the primary focus of this paper.

Behavioral targeting tags consumers by exploiting data stores within the browser that are retained between browsing sessions. Three types of data stores used for behavioral targeting are browser cookies, Web beacons, and Flash cookies. A browser cookie is a small file placed on the client computer. To support behavioral targeting, cookies are loaded with a tag or identifier for tracking.

Another common tagging method is called a Web beacon. Also called a Web bug, clear gif or pixel tag, it is a one by one pixel gif file that is loaded by your browser as an image. It is an image in name only, because it is invisible, and its purpose is to carry in tags and tracking information. Web beacons are stored in your browser cache, a local storage area originally designed to improve page

loading speeds. The http headers for Web beacons contain tag values and other data fields used to facilitate tracking.

A major advantage for Web beacons over cookies is that while browsers offer functionality to control cookies, there is no simple or practical way to block Web beacons. Because Web beacons are disguised as image files, a common component of Web pages, the browser threats them as such. Web beacons are "displayed" on the page (a meaningless act since they are invisible), and stored in the browser cache, along with their tracking information.

Local data stores for browser plug-ins, such as Adobe Flash, are also exploited for behavioral targeting (Dixon, 2007; Soltani, Canty, Mayo, Thomas, & Hoofnagle, 2009). Many e-commerce web sites use the Adobe Flash plug-in for animation and graphics. Adobe Flash uses a local data store that it refers to as shared data objects, but they are also known as Flash cookies.

Next, three case studies of behavioral targeting will be presented. Each case study will be evaluated using the polite software framework. The first case study examines behavioral targeting as conducted on a single web site. The second case study describes the development of alternative tracking mechanisms in response to consumer efforts to block cookies. The third case study presents a measure of the widespread and pervasive use of behavioral targeting, based on evidence from a dataset of over 30,000 users that visited nearly 400,000 unique domains.

Case One: Behavioral Targeting on Levis.com

In order to illustrate the nature of consumer tracking on an individual site, a case study was conducted that examined behavioral targeting within Levis.com, the e-commerce site for the Levis clothing line. An earlier report on this case study can be found at (C. Dwyer, 2009). The results, collected in February 2009, showed the Levis web site loaded a total of nine tracking tags linked to eight third party companies, none of which were named in the privacy policy in effect at the time of data collection.

Levi Strauss & Co. is a privately held company, established in 1853 in San Francisco, California. It main product has been blue jeans, and its brand is identified with American values of rugged individualism. The long association of jeans with the American West reinforces Levi's identification with personal liberty and freedom of choice. When a customer buys Levis jeans, they make an implicit endorsement of these values (J. Sullivan, 2006).

The Levis Privacy Policy

The Levis site provides a privacy policy for the Levis site and those of its related family of websites. The version in place at the time of data collection for this study was updated May 22, 2006, and has since been revised as of October 6, 2009 (Levis.com, 2009). The 2009 as well as the 2006 privacy policy describe the treatment of PII, specifically the use of Secure Socket Layer (SSL) technology to protect personal information. Levis pledges that it does not share personal information without the customer's consent.

In both versions the collection of non-personal or anonymous data is considered a separate category, not specifically protected or subject to affirmative consent. Levis states it collects "Anonymous Information that helps us keep track of information for the purposes of improving our website … [We also] collect Anonymous Information to provide you tailored advertising that we believe you will be much more interested in than randomly-generated advertisements, " (Levis.com, 2009) .

The 2009 policy reports two marketing partners, Razorfish (2009)and GSI Commerce (GSICommerce, 2009), participate in collecting anonymous information from web visitors. Razorfish offers Levis services in support of "tailored advertising," through the use of cookies and Web beacons. GSI Commerce, working along with the analytics company Omniture (2009), offers analytics data to determine the relative popularity of products and areas of the web page. Levis also acknowledges that "GSI also provides all of the administrative and e-commerce services on the Levi's® and Dockers® sites. … GSI is thus exposed to your PII. However, GSI is not authorized to discuss, disclose or make any use

of your PII except as directly necessary to provide us with these services." No other third party service providers are mentioned, although they are indirectly addressed through this language: "We require our trusted business partners, by contract, to protect information obtained from our websites. Our business partners, in turn, require their partners to contractually agree to similar restrictions,"(Levis.com, 2009).

Data Collection Method

For the purpose of clarity, the machine examined for this study will be referred to as the client machine. Data was collected for this study using the following process. The Levis web site was accessed in February of 2009 by the client machine using the Mozilla Firefox browser version 3.0.6. A log of ongoing http headers and resource requests associated with loading the Levis page was collected using the Firefox plug-in TamperData version 10.0.1 (The TamperData Project, 2009). Browser cookies on the client were examined using the Add N Edit Cookies Plug-in (Add N Edit Cookies Project, 2009). Before beginning data collection, the 'clear private data' option was used on Firefox to remove any previous cookies or Web beacons.

[INSERT FIGURE 1 HERE]

To begin data collection, a blank Firefox page was loaded and the address levis.com was directly typed into the address bar. As the main page of the Levis site was accessed, the resource requests generated by the Levis page were logged using TamperData. These logs revealed instances of JavaScript code downloaded to the client machine. The JavaScript code displayed in Figure 1 is from the URL http://switch.atdmt.com/jaction/2008_Levis_Homepage, and originates from Atlas, a behavioral targeting company owned by Microsoft (Atlas, 2009).

This JavaScript code creates seven different one by one image files with tracking information – in other words, seven Web beacons. Several of these beacons connect to competitors of Atlas. For example there is a Right Media Web beacon (number 3, as labeled in figure 1) and one from advertising.com

(number 2). Right Media is owned by Yahoo, Inc., and advertising.com is owned by AOL, Inc. The use of JavaScript code originating from a Microsoft company that plants beacons that link to affiliates of Yahoo and AOL suggests competing advertising networks are cooperating in their data collection techniques.

[INSERT FIGURE 2 HERE]

Next, cookies from Levis were examined for evidence of tagging. Figure 2 shows a cookie named browser_id. The host for this cookie is us.levis.com, and it expires on February 15, 2019. The cookie has a tag value, 62217632133. The TamperData logs revealed a beacon from Omniture, a web analytics company (2009), referencing this tag value. Figure 2 show the tag value from the Levis cookie being passed back to Omniture, along with an extensive list of software installed on the client machine. One potential use of the installed software list is to enable Omniture to retrieve tags from other local data stores, for example from the Silverlight plug-in (Dixon, 2007).

[INSERT FIGURE 3 HERE]

An example of a Web beacon loaded by the Levis site is displayed in Figure 3. This Web beacon, named http://beacon.afy11.net, links to the Adify Corporation (2009). It contains a P3P compact privacy policy in its http header fields (the last line of the response headers, CP= "NOI DSP…"). P3P, an acronym for Platform for Privacy Preferences, is a mechanism for creating machine readable privacy settings developed by the World Wide Web Consortium (www.w3.org, 2009). Compact P3P policies are strings of three letter tokens describing the data handling intentions of a cookie or other data collection tool. This P3P policy states that it will be used to collect non-identified data (NOI), will use a pseudonymous identifier to create a record of browsing activities (PSAa), will keep this information for an indeterminate amount of time (IND), and will collect other types of data that are not currently specified under the P3P protocol (OTC). For a description of all available P3P tokens refer to (P3PWriter, 2009).

Table 1: Summary of Web beacons planted by the Levis site.

Web beacon	*Linked to what company?*	*Has P3P?*	*Collect Identified Data?*	*Used for Tracking?*	*Data Retention?*
tracking.searchmarketing.com	Channel Advisor	Yes	Yes	Yes	IND
beacon.afy11.net	Adify	Yes	No	Yes	IND
leadback.advertising.com	Advertising.com	Yes	No	Yes	BUS
ad.yieldmanager.com/pixel?id=164939&t=2	Right Media	Yes	No	Yes	BUS
bh.contextweb.com	Context Web	Yes	No	Yes	BUS
ad.yieldmanager.com/pixel?id=101690&t=2	Right Media	Yes	No	Yes	BUS
bp.specificclick.net	Specific Media	Yes	No	Yes	BUS
a.tribalfusion.com	TribalFusion	Yes	No	No	BUS
gsiclevi.112.2o7.net	Omniture	Yes	No	Yes	IND

Table 1 provides a summary of nine Web beacons loaded on the client machine from the Levis web site. All nine beacons have P3P policies. These nine beacons link Levis customers to eight digital advertising entities. Eight out of nine of the beacons are used for customer tracking. One beacon, from tracking.searchmarketing.com, collects identified data such as contact information. This beacon comes from Channel Advisor, a firm that provides technology to maximize sales across e-commerce platforms (ChannelAdvisor, 2009). Even though this beacon collects contact information, there is no mention of this company within the Levis privacy policy. This seems to directly contradict Levi's pledge in its privacy policy that it will not share personal information without consent.

An analysis of data retention settings shows three beacons retain data for an indeterminate period of time (IND). Six indicate that data will be retained according to stated business practices (BUS). Although the P3P specifications for the BUS token require that the retention policy must be part of the

provider's privacy policy (P3PWriter, 2009; www.w3.org, 2009), no such data retention information could be found for any of these companies.

Applying Polite Software Framework to Levis Case Study

The results of applying the polite software framework to this case study are as follows. Rule 1 specifies that polite software respects and does not preempt rightful user choices. Levis violates this principle by passing a tag value placed by a first party cookie back to a third party (see figure 2), circumventing any options to block third party cookies.

Rule 2 specifies that polite software reveal itself and its social source. This rule appears to have been violated many times. The Levis sites uses multiple instances of Web beacons, one by one clear images designed to be invisible, thus disguising their social source. Also, there are multiple tracking companies operating on the Levis web site, and their presence is not revealed by the privacy policy.

Rule 3 specifies that polite software helps users make desired choices. Tailored ads are selected for the visitor, based on undisclosed prior browsing behavior. Even if the purpose is benign, tailored advertising violates Rule 3 because it gives the user no choice at all. The Levi's privacy policy state their intent is "to provide you tailored advertising that **we believe** [emphasis added] you will be much more interested in than randomly-generated advertisements," (Levis.com, 2009). The ad is selected in a patronizing way by assuming the advertising network "knows" what ads you want to see.

Rule 4 specifies that polite software remember past user choices. The action of overriding third party cookie blocking ignores past user choices. Through this analysis, we see that behavioral targeting as conducted on the Levis web site does not meet any of criteria of polite software.

Case two – Tracking Mechanisms to Counter Consumer Privacy Efforts

This second case relates to the use of parallel tracking mechanisms in response to consumer efforts to block cookie based tracking. As the general public became aware of tracking through the use of

cookies, more and more consumers deleted or blocked third party cookies. Several studies have found that over 30% of consumers report deleting cookies once a month (Soltani et al., 2009).

Consumer cookie deletion has been the subject of formal study by the online advertising industry. A report from the Atlas Institute entitled "Is the Sky Falling on Cookies," discusses the extent that deleting cookies interferes with targeted advertising (Song, 2005). A study conducted by comScore, Inc. offers an empirical analysis of the impact blocking cookies may have on the accuracy of site-server and ad server metrics (Abraham, Meierhoefer, & Lipsman, 2007).

Behavioral targeting companies are using alternative tracking mechanisms to counter the diminished effectiveness of cookie tracking. One technique has been to shift tracking to other methods that are harder for consumers to manage or block, for example, Flash cookies. Tatto Media, Inc., a behavioral targeting firm (Tatto, 2009), has selected Flash cookies for tracking since they are more likely to remain on a consumer's computer. Lin Miao, the CEO of Tatto Media, explains that their objective has been to "slow the ability of consumers to delete cookies from their computers. Flash cookies are no different than regular cookies in terms of user privacy, but on average remain on a person's computer for more than three months," (L. Sullivan, 2009).

What Tatto Media, and in fact other behavioral targeting companies are doing, is exploiting a security weakness in the browser. Most browsers, such as Firefox or Internet Explorer, enable the installation of helper applications, commonly known as plug-ins. Any plug-in can also have a private data store on the client machine for use by that plug-in. The proliferation of plug-ins, with all their data stores, caches, and temporary files, provides a plethora of locations to place a tracking mechanism. In fact any persistent browser state can be a holding place for a tracking tag (Jackson, Bortz, Boneh, & Mitchell, 2006).

The use of Flash for behavioral targeting has been documented in a study by Soltani et al. (2009). This study found that 54 of the top 100 sites set Flash cookies, and that 34 of these sites stored duplicate

tracking information simultaneously on Flash cookies and browser cookies. The researchers found only four of the top 100 sites even mentioned the use of Flash cookies. The findings from this study show that the use of Flash cookies is widespread, and are in many cases designed to "back up" browser cookies. This duplicate tracking mechanism provides a way to overcome cookie deletions, "thus subverting the user's attempt to prevent tracking," (Soltani et al., 2009, p. 4).

This study also demonstrated Flash cookies were used to circumvent the formal opt-out anti-tracking mechanism established by the Network Advertising Initiative (NAI). NAI members pledge to refrain from tracking if a consumer loads an 'opt-out' cookie into their browser. However this study found a Flash cookie was used to "re-spawn" a tracking cookie even when the user had opted out of tracking through the NAI opt-out cookie. In response to negative publicity generated by the release of this study, the behavioral targeting firm QuantCast announced it was stopping the practice of using Flash cookies to re-spawn browser cookies (Singel, 2009).

Application of Polite Software Framework to Flash Cookie Tracking

Using Flash cookies to re-create browser cookies clearly violates Rule 1 by preempting user choice to block tracking. This intent to preempt user choice is apparent in both the comments by leaders of behavioral targeting firms, and by the "re-spawning" of browser cookies. This practice also violates Rule 2, because the study by Soltani et al. found that most sites did not acknowledge Flash cookies in their privacy policy. The selection of a technology that users have a hard time managing violates Rule 3, because helps users make desired choices. The re-spawning of cookies violates Rule 4, by overriding past user choices, by not respecting the user choice to opt-out of tracking.

Case three – Ghostery and The KnowPrivacy Project

This case study presents the findings of the KnowPrivacy project, conducted at the UC Berkeley School of Information (Gomez, Pinnick, & Soltani, 2009). This study presents an extensive survey of the

state of online privacy. An important source for the project came from data collected by a Firefox plug-in called Ghostery (Ghostery, 2009).

The Ghostery plug-in examines web pages and shows any hidden Web bugs found in a page (for example, see figure 4). It has an optional 'GhostRank' feature that forwards a record of all discovered Web bugs to a central database maintained by Ghostery. GhostRank collects data across a wide swath of the web through a method known as crowd sourcing. Crowd sourcing, a technique that evolved within the open source community, amplifies the acts of individuals, supporting the efforts of many users carrying out similar tasks, channeling the results towards a particular objective (J. Howe, 2006).

[INSERT FIGURE 4 HERE]

Data collected by GhostRank during March 2009 was used to examine the use of Web bugs on the top 100 web sites. This dataset contained approximately 300,000 users, of which 10-15% (30,000-45,000 users) participated in the GhostRank reporting feature. While these users reported on 393,829 unique domains, this analysis focused on the top 100 sites.

The dataset revealed that Web bugs are ubiquitous on the web. The researchers note "this is troubling because users are less likely to know of Web bugs, and effective controls for this tracking technology are lacking, " (Gomez et al., 2009, p. 4). At least one Web bug was found on each of the top 50 sites during the data collection period. Many others had dozens, and the site blogspot.com topped the list with 100 identified Web bugs.

This study also revealed that several tracking companies had a one Web bug on 50 or more of the top 100 sites, including Microsoft Atlas, Omniture, Quantcast, and DoubleClick. The company with the most extensive distribution is Google, with Web bugs on 92 of the top 100 sites, and on 88% of the data set of 400,000 unique domains within the dataset.

Application of Polite Software Framework to KnowPrivacy Project

The KnowPrivacy project demonstrates the widespread distribution of tracking mechanisms from multiple advertising networks. Applying Rule 1, the scale of the tracking preempts user choice. There are so many ways to be tracked it is impossible to find and block all of them. The scale of tracking also violates Rule 2, because these sites are not declaring the social source of dozens of tracking mechanisms. It also violates Rule 3, because the duplication and proliferation of tracking mechanisms makes it very difficult to avoid tracking. The scale of tracking also violates Rule 4, because an effort to opt-out of one advertising network does nothing about tracking from a different advertising network.

Discussion of Polite Software and Behavioral Targeting

The application of the polite software framework to these three case studies reveals that behavioral targeting in many ways is impolite. Consumers expect sales staff to be polite, and they also expect the technology that supports e-commerce to be polite. Just as impolite sales staff can drive away customers, so can the impolite actions of behavioral targeting anger consumers and weaken e-commerce.

In polite interaction, control is shared, and "*the interaction locus of control* passes back and forth between the parties," (Whitworth, 2005). Giving control back is being polite, and politeness is more than kindness. An imposed good is not polite, because it denies the other party a choice (Waldo, Lin, & Millett, 2007; Whitworth, 2005, 2009). This is particularly relevant to the justification that targeted advertising is better aligned with your interests. Even if targeted ads are "good for you," this is not polite, because it takes away your choice. Instead it is paternalistic, because it tries to influence your actions or choice of products. Paternalism is defined as "practice in which the values of the another are imposed upon the person most affected by the decisions to be made, without heeding that person's own values or power to make decisions that directly affect them," (Mifflin, 2004).

When a software is not polite, Whitworth describes this as a "social error," which has the potential to drive away users (Whitworth, 2009). So the issue is not the intent or benevolence of behavioral targeting, it is instead the degree of politeness with which it treats online customers.

An examination of behavioral targeting practices through the lens of the polite software demonstrates that these practices can undermine consumer trust in e-commerce. Whitworth credits the success of eBay, Google, Amazon, WikiPedia, and Facebook to the politeness inherent in these site's interactions with its visitors (Whitworth, 2009). The collection, interpretation, and personalization of consumer behavior has been a transformative component of many successful e-commerce enterprises. However if this data collection is conducted in a clandestine and deceptive way, it can damage the underlying business model, and destroy trust in a brand.

A nationally representative telephone survey conducted in 2009 found that roughly two-thirds of Americans object to online tracking by advertisers (Turow, King, Hoofnagle, Bleakley, & Hennessy, 2009). When subjects were asked about specific techniques used to select ads, the percentage objecting rose even higher. For example, 75% say it is ***not ok*** to tailor ads based on the web site you are visiting, 87% say it is ***not ok*** to tailor ads based on past online browsing, and 89% say it is ***not ok*** to tailor ads based on your offline activity (Turow et al., 2009).

As behavioral targeting has gained more attention, users have begun to arm themselves with cookie-blocking, anti-tracking plug-ins and tools, such as Ghostery, which displays tracking mechanisms (Gomez et al., 2009), TrackMeNot, which interferes with tracking by corrupting cookie values and adding noise to tracking data (D. C. Howe & Nissenbaum, 2009), or the Firefox plug-in Taco, which blocks tracking from 90 separate advertising networks (Witte, 2009). This escalating arms race between consumer and behavioral targeting is a sign that behavioral targeting can cause more harm than good. "Customer conflict is not the norm for online businesses, and should not be for online business," (Whitworth, 2005, p. 362).

The negative opinion of tailored advertising captured by this survey is consistent with empirical evidence of user discomfort with personalization captured in a study conducted by Stoecklin-Serino and Paradice (2009). They reported that "personalization was found to have a significant and negative impact on trusting beliefs in all four trials," (p. 19).

Personalization was also found to diminish trust in an earlier study by Alpert et al. (2003). This study found "unenthusiastic user attitudes toward system attempts to infer user needs, goals, or interests and to thereby provide user-specific adaptive content…Users expressed their strong desire to have full and explicit control of data and interaction …The clearest result to emerge from our studies is users' fervent desire to be *in control*," (Alpert et al., 2003).

A result from this study particularly relevant to behavioral targeting is that subjects did not want information *implicitly* collected by the system to become part of their personal profile. Implicit information included "user interests, user goals, navigation paths the user has traveled, or any other data regarding the user that is inferred by the system based on." The participants in this study indicated they wanted only information *explicitly* provided by them to be remembered by the system: 'I want the stored information to be based on what I told you, not what you think I've said,'" (Alpert et al., 2003p. 385).

Besides being impolite, deceptive tracking practices can directly reduce trust. An study found trust is particularly damaged by deceptive behavior. Schweitzer, Hershey and Bradlowc (2006) reported that "trust harmed by deception never fully recovers. Unlike untrustworthy actions alone, untrustworthy actions combined with deception causes enduring harm to trust," (Schweitzera, Hershey, & Bradlowc, 2006, p. 19)

Behavioral targeting has been described by Cindy Cohn, the legal director of the Electronic Frontier Foundation, as "the surveillance business model," (Cohen, 2009). Behavioral targeting without consent threatens the autonomy of consumers, and can undermine the trust and expectations of benevolence that customers associate with a name brand. "Politeness is not about forcing users to buy,

which is anti-social, but about improving the seller-customer relationship which leads to sales by giving customers choice, which is social," (Whitworth, 2009).

Summary and Recommendations

The consumer tracking being conducted with tools such as browser cookies, Web beacons, and Flash cookies is largely invisible during ordinary Web browsing. The image files used for Web beacons cannot be seen on the page, and their size is kept small to minimize any performance impact that might make them noticeable. One defense for behavioral targeting is that the information being collected is anonymous. This defense does not address the one sided power that tracking can gives a marketer to influence an anonymous but very real consumer with their online purchases.

The Future of Privacy Forum (2009), a privacy advocacy group, has recommended an "affirmative consent model" for behavioral targeting, meaning that consumers explicitly give consent (i.e., opt-in) to data collection and data sharing within advertising networks. On February 12, 2009 the FTC released new recommendations for behavioral targeting to increase the transparency of targeted ads (FTC, 2009). In October 2009 the Council of the European Union approved regulatory changes that sharply restrict the use of cookies. The new regulations state that cookies without user consent would only be allowed when they are "strictly necessary" to provide a service "explicitly requested" by the user such as storing shopping cart information on e-commerce sites (Taylor, 2009).

There are forces taking shape that will alter the current behavioral targeting landscape. E-commerce sites should act quickly to restore consumer trust by providing more transparency to data collection practices, and implementing mechanisms of explicit consent for behavioral targeting. As FTC Chairman Jon Leibowitz has proclaimed, "People should have dominion over their computers … The current 'don't ask, don't tell' in online tracking and profiling has to end," (Story, 2007).

References

Abraham, M., Meierhoefer, C., & Lipsman, A. (2007). *The Impact of Cookie Deletion on the Accuracy of Site-Server and Ad-Server Metrics: An Empirical Comscore Study*. Retrieved October 14, 2009, from http://www.comscore.com/Press_Events/Presentations_Whitepapers/.

Add N Edit Cookies Project. (2009). Retrieved February 21, 2009, from http://addneditcookies.mozdev.org/.

Adify. (2009). *Vertical Ad Solutions by Adify*. Retrieved February 21, 2009, from http://www.adify.com/.

Alpert, S. R., Karat, J., Karat, C.-M., Brodie, C., & Vergo, J. G. (2003). User Attitudes Regarding a User-Adaptive eCommerce Web Site. *User Modeling and User - Adapted Interaction, 13*(4), 373-396.

Atlas. (2009). *Atlas Solutions*. Retrieved February 21, 2009, from http://www.atlassolutions.com/index.aspx.

Benbasat, I., Gefen, D., & Pavlou, P. A. (2008). Special Issue: Trust in Online Environments. *Journal of Management Information Systems, 24*(4), 5-11.

ChannelAdvisor. (2009). *ChannelAdvisor*. Retrieved February 23, 2009, from http://www.channeladvisor.com/.

Clifford, S. (2009). "An Interview With David Vladeck of the F.T.C." Media Decoder Blog, retreived October 14, 2009, from http://mediadecoder.blogs.nytimes.com/2009/08/05/an-interview-with-david-vladeck-of-the-ftc/.

Cohen, N. (2009, February 16, 2009). As Data Collecting Grows, Privacy Erodes. *The New York Times,* p. B3.

Dixon, P. (2007, November 2, 2007). *The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation*. Retrieved February 15, 2009, from http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf.

Dwyer, C. (2009). Behavioral Targeting: A Case Study of Consumer Tracking on Levis.com, *America's Conference on Information Systems*. San Francisco, CA.

Dwyer, F. R., Schurr, P. H., & Oh, S. (1987). Developing Buyer-Seller Relationships. *The Journal of Marketing, 51*(2), 11-27.

Flanagan, M., Howe, D. C., & Nissenbaum, H. (2008). Embodying Values in Technology: Theory and Practice. In J. van den Hoven & J. Weckert (Eds.), *Information Technology and Moral Philosophy* (pp. 322-353). Cambridge: Cambridge University Press.

FTC. (2000, June 2000). *Online Profiling: A Report to Congress*. Retrieved February 15, 2009, from http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf.

FTC. (2009, February 12, 2009). *FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising*. Retrieved February 15, 2009, from http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

Fukuyama, F. (1995). *The social virtues and the creation of prosperity*. New York: Free Press.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in Online Shopping: An Integrated Model. *MIS Quarterly, 27*(1), 51-90.

Ghostery. (2009). *Ghostery Home Page*. Retrieved May 18, 2009, from http://www.ghostery.com/.

Gomez, J., Pinnick, T., & Soltani, A. (2009). *KnowPrivacy*. Retrieved October 14, 2009, from knowprivacy.org.

GSICommerce. (2009). *GSI Commerce*. Retrieved November 13, 2009, from http://www.gsicommerce.com/.

Howe, D. C., & Nissenbaum, H. (2009). *TrackMeNot*. Retrieved November 13, 2009, from http://mrl.nyu.edu/~dhowe/trackmenot/.

Howe, J. (2006). The Rise of Crowdsourcing. *Wired, 14,* 1-12.
Jackson, C., Bortz, A., Boneh, D., & Mitchell, J. C. (2006). *Protecting browser state from web privacy attacks.* Paper presented at the Proceedings of the 15th international conference on World Wide Web, Edinburgh, Scotland.
Kelley, S. W. (1992). Developing customer orientation among service employees. *Journal of the Academy of Marketing Science, 20*(1), 27-36.
Levis.com. (2009). *Levi Strauss & Co.'s Privacy Policy*. Retrieved November 4, 2009, from http://us.levi.com/helpdesk/index.jsp?display=safety&subdisplay=privacy&clickid=botnav_privacy_img.
Mankiw, W. G. (2000). *Principles of Economics*. Florence, KY: Southwest College Publishing.
Metzger, M. J. (2004). Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce. *Journal of Computer-Mediated Communication, 9*(4).
Mifflin, H. (Ed.). (2004). *The American Heritage Dictionary of the English Language* (Fourth Edition ed.). New York: Houghton Mifflin Company.
Miller, C. A. (2004). Human-Computer Etiquette: Managing Expectations with intentional agents. *Communications of the ACM, 47*(4), 30-34.
NAI. (2009). *Network Advertising Initiative*. Retrieved February 15, 2009, from http://www.networkadvertising.org/index.asp.
Nass, C. (2004). Etiquette equality: exhibitions and expectations of computer politeness. *Communications of the ACM, 47*(4), 35-37.
Nass, C., Steuer, J., & Tauber, E., R. (1994). *Computers are social actors.* Paper presented at the Proceedings of the SIGCHI conference on Human factors in computing systems: celebrating interdependence, Boston, Massachusetts, United States.
Omniture. (2009). *Online Business Optimization by Omniture*. Retrieved February 21, 2009, from http://www.omniture.com/en/.
P3PWriter. (2009). *P3P Compact Policies*. Retrieved February 21, 2009, from http://www.p3pwriter.com/LRN_111.asp.
Petronio, S. (2002). *Boundaries of Privacy: Dialectics of Disclosure*. Albany: State University of New York Press.
Platteau, J.-P. (1994). Behind the market stage where real societies exist--Part II: The role of moral norms. *Journal of Development Studies, 30*(4), 753.
Razorfish. (2009). *Razorfish: The Agency for Marketing, Experience & Enterprise Designs for the Digital World*. Retrieved February 23, 2009, from http://www.razorfish.com/.
Schweitzer, M. E., Hershey, J. C., & Bradlowc, E. T. (2006). Promises and lies: Restoring violated trust. *Organizational behavior and human decision processes, 10*(1), 1-19.
Schweitzera, M. E., Hershey, J. C., & Bradlowc, E. T. (2006). Promises and lies: Restoring violated trust. *Organizational behavior and human decision processes, 10*(1), 1-19.
Singel, R. (2009). "Flash Cookie Researchers Spark Quantcast Change." Wired, retreived November 4, 2009, from http://www.wired.com/epicenter/2009/08/flash-cookie-researchers-spark-quantcast-change/.
Soltani, A., Canty, S., Mayo, Q., Thomas, L., & Hoofnagle, C. J. (2009). *Flash Cookies and Privacy*. Retrieved October 14, 2009, from http://ssrn.com/paper=1446862
Song, Y.-B. (2005). *Is the Sky Falling on Cookies? Understanding the Impact of Cookie Deletion on Web Metrics*. Retrieved October 14, 2009, from http://www.atlassolutions.com/uploadedFiles/Atlas/Atlas_Institute/Published_Content/AIDMIOnCookieDeletion.pdf.

Stoecklin-Serino, C., & Paradice, D. (2009). An Examination of the Impacts of Brand Equity, Security, and Personalization on Trust Processes in an E Commerce Environment. *Journal of Organizational and End User Computing, 21*(1), 1-36.

Story, L. (2007, November 2, 2007). FTC Member Vows Tighter Control of Online Ads. *The New York Times*.

Sullivan, J. (2006). *Jeans: a cultural history of an American icon*. New York: Gotham Books.

Sullivan, L. (2009). "Moving Flash Cookies Into Direct-Response BT." Behavioral Insider, retreived October 15, 2009, from http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=113594.

The TamperData Project. (2009). Retrieved February 21, 2009, from http://tamperdata.mozdev.org/.

Tang, Z., Hu, Y. J., & Smith, M. D. (2008). Gaining Trust Through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor. *Journal of Management Information Systems, 24*(4), 153-173.

Tatto. (2009). *Tatto Media*. Retrieved November 5, 2009, from http://www.tattomedia.com/.

Taylor, M. (2009). "Europe Approves New Cookie Law." WSJ Blogs, retreived November 13, 2009, from http://blogs.wsj.com/digits/2009/11/11/europe-approves-new-cookie-law/.

Turel, O., Yuan, Y., & Connelly, C. E. (2008). In Justice We Trust: Predicting User Acceptance of E-Customer Services. *Journal of Management Information Systems, 24*(4), 123-151.

Turow, J., King, J., Hoofnagle, C. J., Bleakley, A., & Hennessy, M. (2009). *Contrary to what marketers say, Americans Reject Tailored Advertising and Three Activities That Enable It*. Retrieved October 14, 2009, from http://graphics8.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf.

Waldo, J., Lin, H. S., & Millett, L. I. (2007). *Engaging Privacy and Information Technology in a Digital Age*. Washington, DC: National Academies Press.

Whitworth, B. (2005). Polite Computing. *Behavior and Information Technology, 24*(5), 353-363.

Whitworth, B. (2009). Politeness as a Social Software Requirement. *International Journal of Virtual Communities and Social Networking, 1*(2), 65-84.

Williamson, O. (1985). *The Economic Institutions of Capitalism*. New York: The Free Press.

Witte, D. (2009). *Targeted Advertising Cookie Opt-out (TACO)*. Retrieved November 13, 2009, from http://taco.dubfire.net/.

www.futureofprivacy.org. (2009, November 26, 2008). *The Future of Privacy Forum*. Retrieved February 16, 2009, from http://www.futureofprivacy.org/.

www.w3.org. (2009). *P3P - The Platform for Privacy Preferences*. Retrieved February 21, 2009, from http://www.w3.org/P3P/.

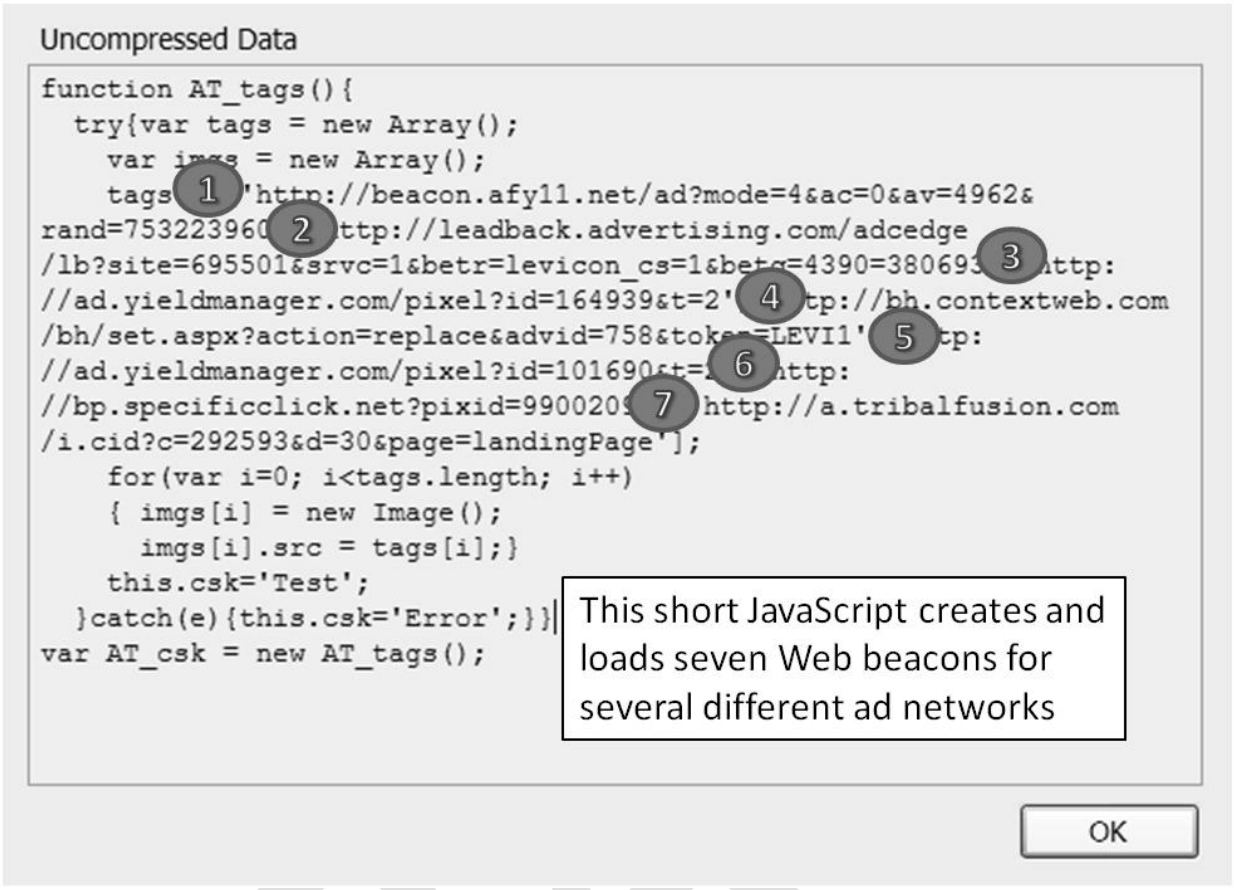

Figure 1: This short JavaScript downloads from the Levis site, and quickly creates seven Web beacons for various advertising networks, including Yield Manager, TribalFusion, and Advertising.com.

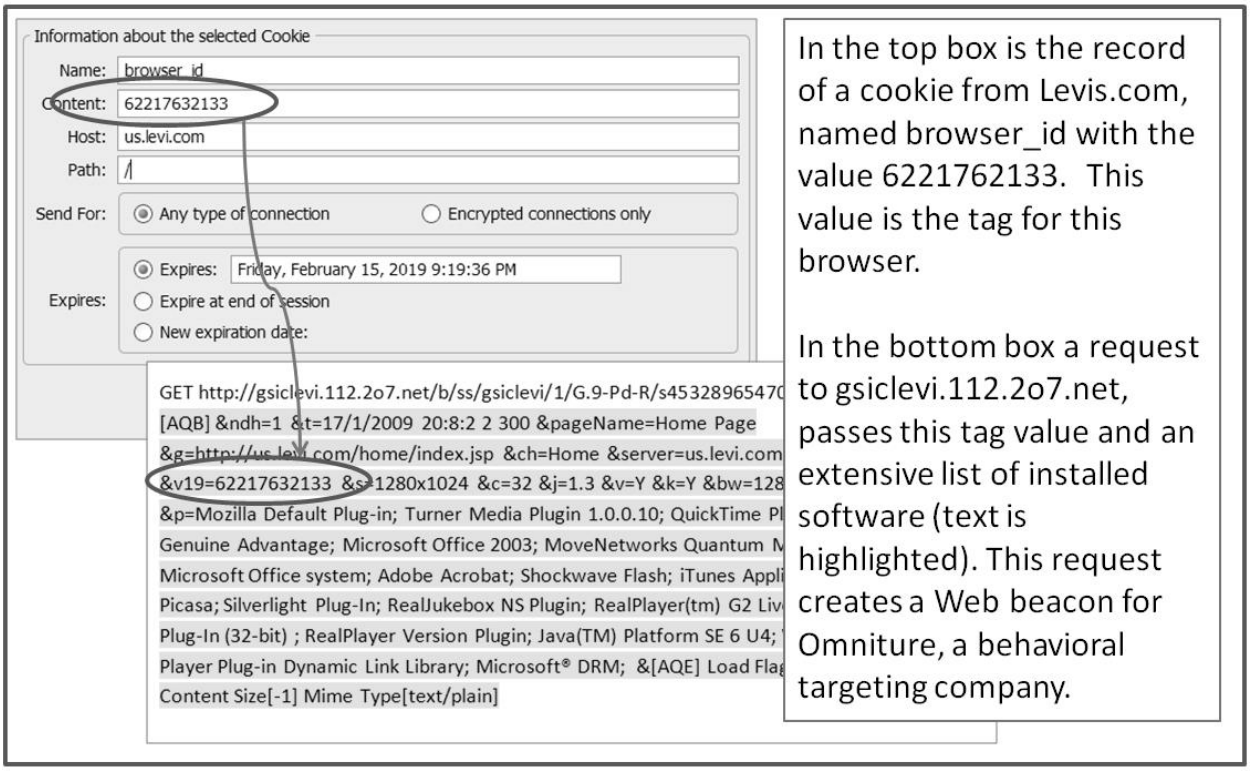

Figure 2: The tag value from a cookie is passed back to Omniture using a Web beacon.

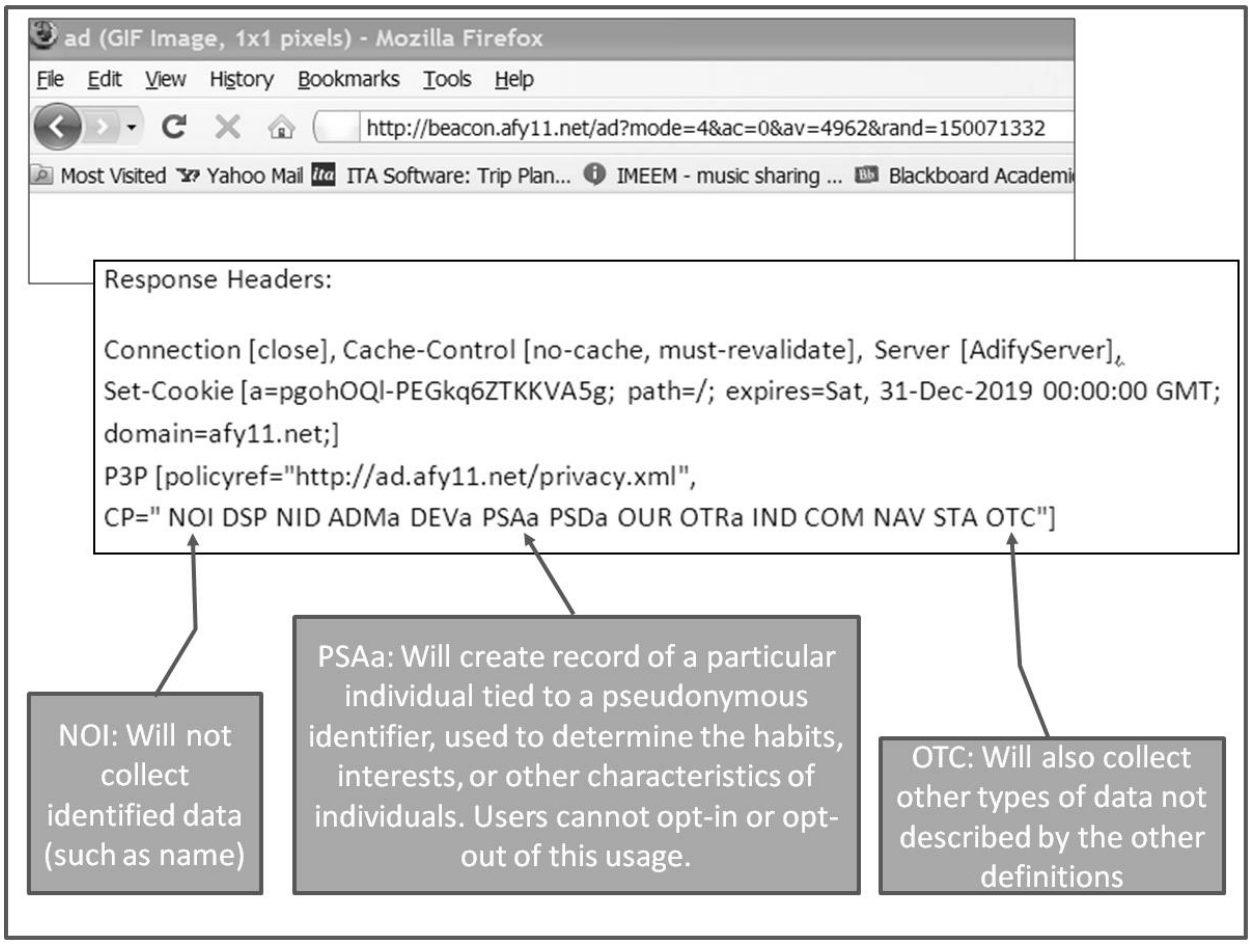

Figure 3: Analysis of data collection uses for this Web beacon.

Figure 4: The Ghostery tool identifies four Web bugs on a page from the Huffington Post.