Behavioral Targeting: A Case Study of Consumer Tracking on Levis.com

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. The vast majority of data is collected anonymously, i.e., not linked to a person's name. However, behavioral targeting does create digital dossiers on consumers with the aim of connecting browsing activity to a tagged individual. This tagging is largely invisible to consumers, who are not asked to explicitly give consent for this practice. By using data collected clandestinely, behavioral targeting undermines the autonomy of consumers in their online shopping and purchase decisions. In order to illustrate the nature of consumer tracking, a case study was conducted that examined behavioral targeting within Levis.com, the e-commerce site for the Levis clothing line. The results show the Levis web site loads a total of nine tracking tags that link to eight third party companies, none of which are acknowledged in the Levis privacy policy. Behavioral targeting, by camouflaging the tracking of consumers, can damage the perceived trustworthiness of an e-commerce site or the actor it represents. The risks behavioral targeting presents to trust within e-commerce are discussed, leading to recommendations to reestablish consumer control over behavioral targeting methods.

Keywords

Trust, Privacy, Behavioral Targeting, Web beacons, E-Commerce, Risk Analysis

INTRODUCTION

Behavioral targeting involves the collection of information about a consumer's online activities in order to deliver advertising targeted to their potential upcoming purchases. It is conducted by companies that are 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.

In a report released in 2000, the Federal Trade Commission (FTC) offers the following scenario describing behavioral targeting. 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 logging her airline shopping behavior with the advertising network.

In the years since the FTC released that report, behavioral targeting has increased in scope and sophistication. The iWatch web crawler, a tool developed to document online tracking methods, has shown about six percent of Web sites in the US deploy third party cookies, and 36 % deploy Web beacons (Jensen, Sarkar, Jensen and Potts, 2007). While these results show the use of behavioral targeting is widespread, the nature of behavioral targeting within a specific site has not been examined in depth. Therefore, this study was conducted to look at behavioral targeting as carried out on the Levis.com web site.

The rest of the paper is organized as follows. The next section describes the technology used in behavioral targeting. That is followed by a review of relationship between trust and privacy. The next section presents the results of a study of behavioral targeting on the Levis site. This is followed by a discussion of the risks to Levis and e-commerce sites in general. The final section offers recommendations for addressing these risks by changing the nature of behavioral targeting.

OVERVIEW OF BEHAVIORAL TARGETING TECHNOLOGY

Behavioral targeting customizes messages to individual consumers based on their specific shopping interests, and characteristics like gender, age, and ethnicity. 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.

Advertising networks establish relationships with partner Web sites, collect visitor browsing data, and serve ads matched by algorithm to information known about the online visitor. Some of the largest companies offering these services include Advertising.com, Inc., Akami Technologies, Blue Lithium, TACODA, 24/7 Real Media, Tribal Fusion, DoubleClick, and Atlas Solutions (2009g).

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 cunsumers.

Behavioral targeting tags consumers by exploiting persistent browser state. Three types of persistent state 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.

Local data stores for browser plug-ins, such as Adobe Flash, are also exploited by behavioral targeting (Dixon, 2007). 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. In fact, Adobe offers an online tutorial on how to assign tags to animation files in order to track interactions with Flash movies (2009l).

Growing awareness of privacy risks has led to an increase in blocking cookies. This diminishes the effectiveness of cookies for behavioral targeting, so that other methods have been expanded (Dixon, 2007). A common practice of advertising networks is to deploy all three methods at the same time – tagging each consumer with browser cookies, Web beacons, and Flash cookies. This belts and suspenders process of consumer tracking allows advertising networks to "invisibly engage in cross-domain tracking of [web] visitors," (Jackson, Bortz, Boneh and Mitchell, 2006).

Combining multiple methods of data collection offers advertisers a richer picture of consumer behavior. As the FTC has noted, advertisers are eager to expand data collection to new platforms such as the mobile device (2009c). The goal for targeting, according to Keith Johnson, vice-president of product management at i-Behavior, Inc., is to "connect online, offline (for example, catalog) and in-store retail purchase behavior" so that tracking is continuous, comprehensive, and complete (Leggiere, 2009).

THE RELATIONSHIP BETWEEN PRIVACY AND TRUST

Research has shown that trust is an important component of e-commerce, and that lack of trust leads to lost customers and business opportunities (Gefen, Karahanna and Straub, 2003). Trust 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. Petronio describes privacy management as a dialectical process, where privacy boundaries expand or contract based on trust in the other party. Trust and privacy have a complex, but mutually dependent relationship. Trust can influence privacy management, and privacy breaches, which Petronio refers to as privacy boundary turbulence, can damage trust (Petronio, 2002).

One difficulty for e-commerce sites in managing trust and privacy is lack of agreement on the meaning of privacy. While notions of privacy have persisted for centuries and are found in cultures around the globe, a consensus on a precise definition has been elusive. Academic works on privacy focus on either providing a definition for privacy, or explaining why privacy

should be valued. A focus on definitions provides a descriptive account of privacy, and a focus on value leads to a normative account of privacy (Waldo, Lin and Millett, 2007).

Within e-commerce the most influential account of privacy has been Westin's definition: "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extend information about them is communicated to others," (Westin, 1967). Here, privacy equals control over information, and private information "belongs" to an individual, as a type of property right. Like other property, an individual can keep (conceal) or dispose of privacy (disclose or make public). The conceptualization of privacy as a property right has been quite influential within e-commerce privacy policies (Solove, 2004).

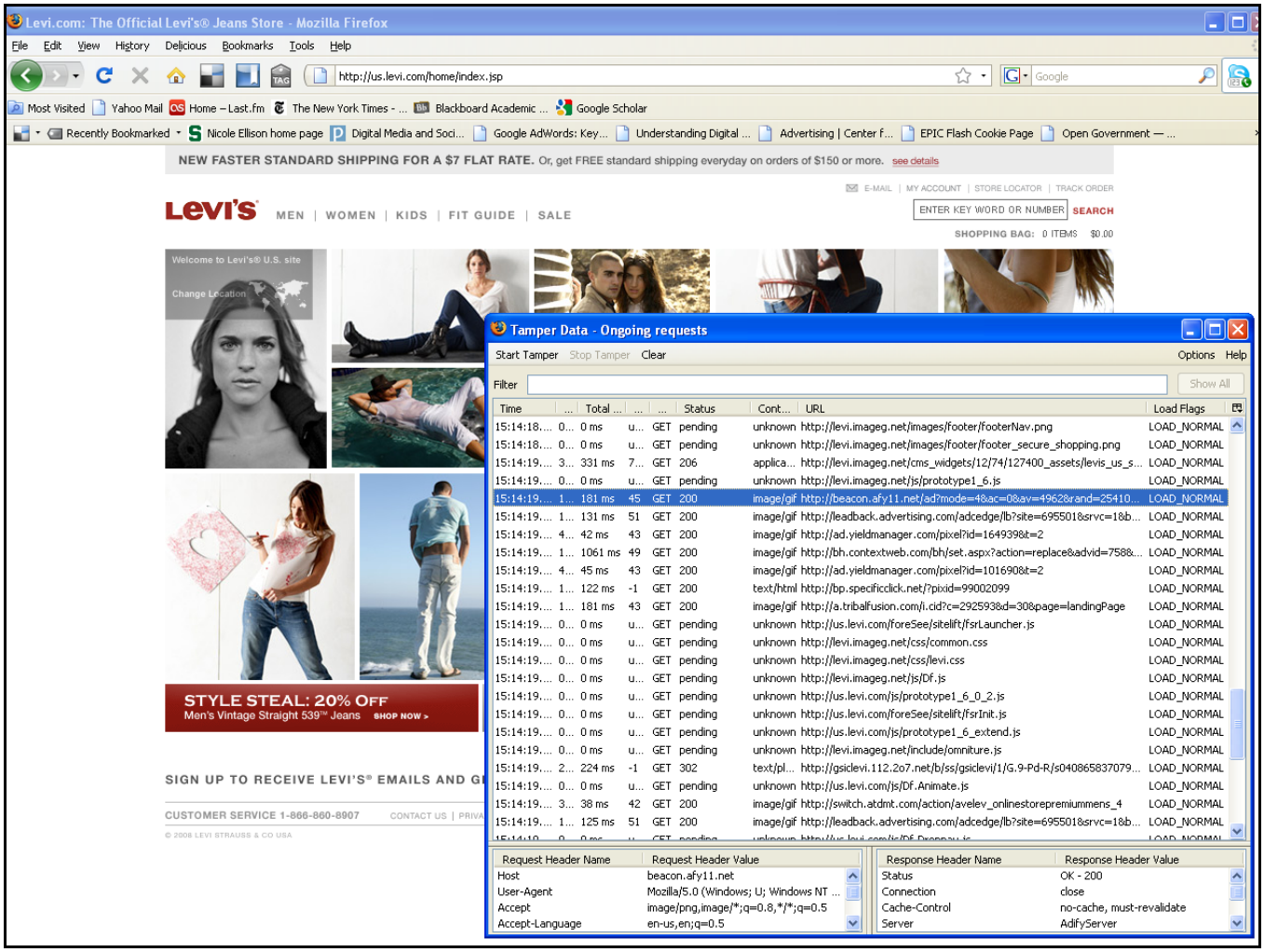

Figure 1: The Levis Home Page, and log of resource requests associated with loading that page.

Problems with defining privacy as control

Defining privacy as control over information has been extremely problematic. First of all, people have already lost control of existing digital data, with more piling up every day. Any comprehensive solution to deliver individual control over past, present and future information would be faced with an intractable problem (Ackerman, 2000). Secondly, it treats all pieces of information as discreet, independent data elements to be managed one by one. Following this analysis, people set up controls for their email address, different controls for their credit card number, and other controls for their gender. This interpretation of privacy is used to split apart a person's digital trail into PII and non-PII. Within e-commerce, formal privacy mechanisms are only concerned with PII. Issues of informed consent, adequate data security, and rules for data sharing are only explicitly spelled out for PII. Everything else collected about online browsing, including sensitive items such as location (obtained from

your IP address), what online articles you read, and what keywords you enter into a search engine are excluded from official considerations of online privacy. Under the control definition of privacy, you only need to control your information if you can be identified. As long as you are treated anonymously, then you have no privacy concerns.

Anonymity does not equal privacy

The problem with the equating anonymity with privacy becomes apparent by considering the instrumental value of privacy. For example, privacy is valued because it protects the autonomy of the individual, and preserves independence and free choice in decision processes. Another instrumental value associated with privacy is that it contributes to fairness. Privacy can help ensure a level playing field for information flow between two parties in a transaction. Without privacy, it would be easier for wealthier, more powerful parties to obtain information about the other and gain an advantage (Waldo, Lin et al., 2007). By considering the value of autonomy and fairness, we see tracking consumers anonymously is an issue because it undermines their autonomy.

Economic perspectives on privacy have also been influential. One school of economic thought holds that privacy restricts information flow, interfering with the efficient workings of the market (Waldo, Lin et al., 2007). This leads to considering privacy as something consumers can trade for some other economic good. However, there are broader consequences from trading away privacy. For example, an employee browsing the web at work may sign up for a free service in exchange for tracking her online behavior. This data is of interest not only to online marketers, but her company's competitors as well. Behavioral targeting here functions as a powerful conduit for industrial espionage (Conti, 2009).

A normative approach provided by Nissenbaum holds that information flow is governed by social norms highly dependent on context (Waldo, Lin et al. 2007). So for example, information flow can differ within a health context, among friends, or in a public setting. Nissenbaum argues privacy should be conceptualized as a relational and social property (Solove 2007). The conception of privacy as an individual right makes it difficult to implement it within an online social environment. The fundamental problem of the information privacy paradigm is that it reinforces an individualistic interpretation of privacy, and creates a software requirement of control that is a fundamentally intractable problem (Ackerman 2000). It has also been used to justify pervasive tracking of anonymous but very real consumers.

LEVIS.COM: A CASE STUDY OF BEHAVIORAL TARGETING IN ACTION

The web site for this case study is Levis.com, an e-commerce shopping site for the Levis clothing line. 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 (Sullivan, 2006).

The Levis Privacy Policy

The Levis site provides a privacy policy, "Levi Strauss & Co.'s Commitment to Privacy," last updated May 22, 2006 (2009f). It describes 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.

However, the collection of non-personal or anonymous data is considered a separate category, not specifically protected or subject to affirmative consent. Levis states it will "automatically collect and store certain other information to enable us to analyze and improve our websites and to provide our customers with a fulfilling online experience. For example, we collect your IP address, browser information and reference site domain name every time you visit our site. We also collect information regarding customer traffic patterns and site usage."

The policy reports a third party advertising company, Avenue A, collects "anonymous information about your visits to our website. This is primarily accomplished through the use of a technology device, commonly referred to as a Web beacon . . . Avenue A may use anonymous information about your visits to this and other websites in order to provide ads about goods and services of interest to you." The policy also describes an unnamed third party that places Web beacons on the site to measure use of the site. The policy concludes by addressing the issue of consent: "By using our website, you're agreeing to let us collect and use your non-personal information as we describe in this Privacy Policy,"(2009f). There are no references to other third party service providers that may be collecting data from Levis customers.

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 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 (2009k). Browser cookies on the client were examined using the Add N Edit Cookies Plug-in (2009a). Before beginning the data collection, the 'clear private data' option was used on Firefox to remove all previous cookies or Web beacons.

Figure 1 shows a screen shot with the Levis home page, and a log of resource requests recorded by TamperData. TamperData logs the name and type of resource requested, status information, the contents of the http Request Header (originating on the client and sent to the server) and the contents of the http Response Header (sent by the server along with the resource requested).

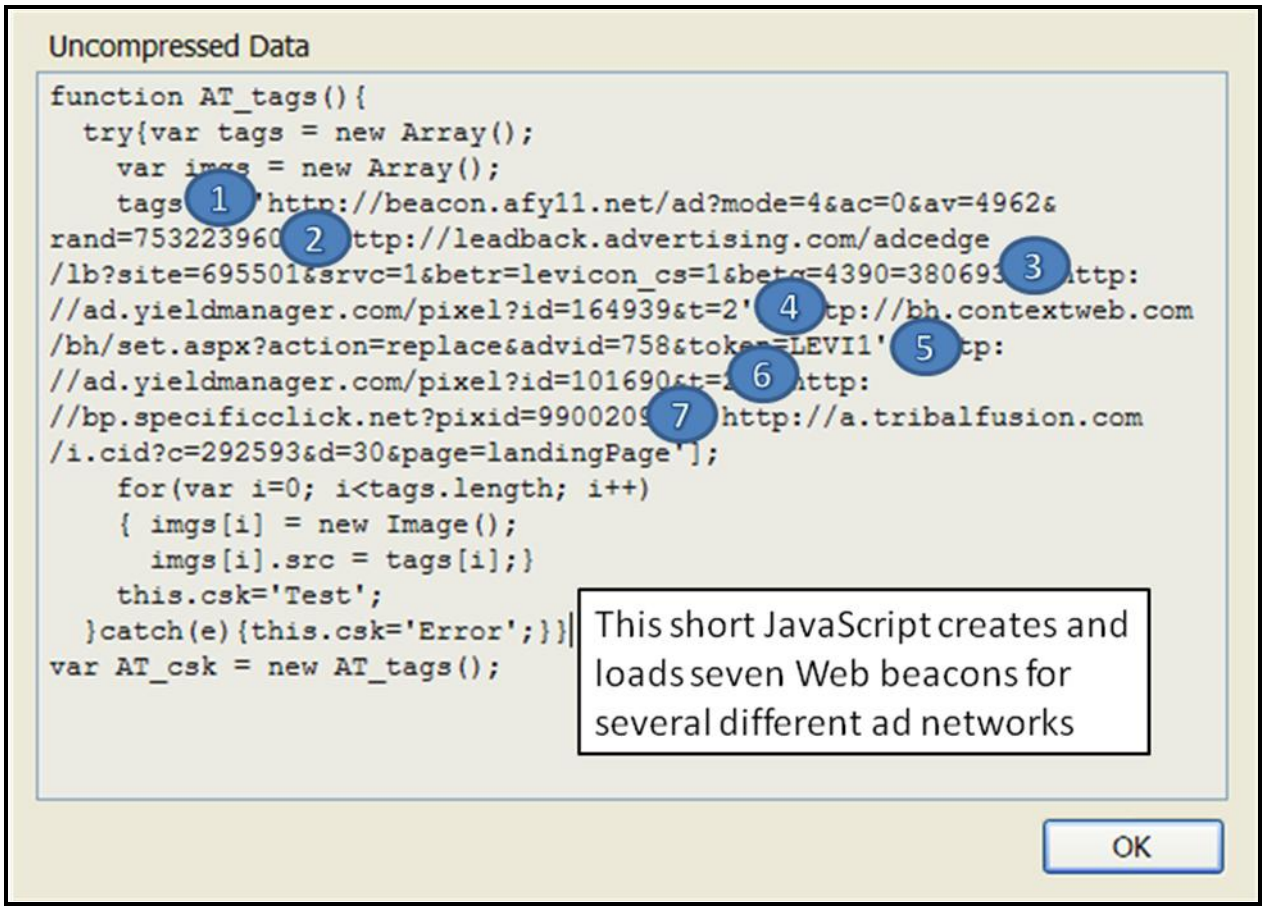

Figure 2: This short JavaScript downloads from the Levis site, and quickly creates seven Web beacons for various advertising networks, including Yield Manager, TribalFusion, and Advertising.com.

To begin data collection, the main page of the Levis site was accessed, and the resource requests generated by the Levis page were recorded using TamperData. These logs revealed instances of JavaScript code downloaded to the client machine. The JavaScript code displayed in Figure 2 comes from the URL http://switch.atdmt.com/jaction/2008_Levis_Homepage, and originates from Atlas, a behavioral targeting company (2009b). This 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 TribalFusion Web beacon (number 7, as labeled in figure 2) and one from advertising.com (number 2). This suggests competing advertising networks are cooperating in their data collection techniques.

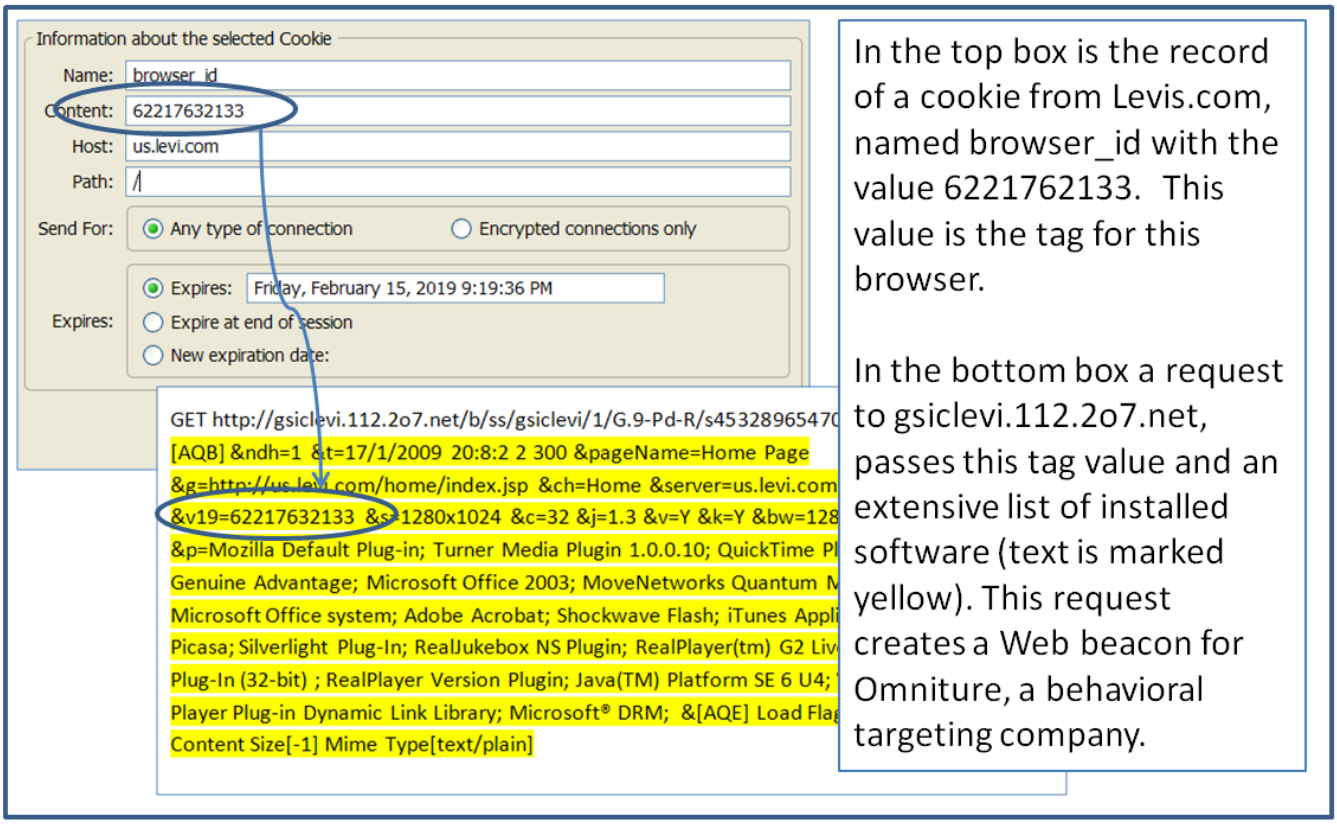

Figure 3: The tag value from a cookie is passed back to Omniture using a Web beacon.

Next, cookies from Levis were examined for evidence of tagging. Figure 3 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 (2009n), referencing this tag value. Figure 3 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).

An example of a Web beacon loaded by the Levis site is displayed in Figure 4. This Web beacon, named http://beacon.afy11.net, links to the Adify Corporation (2009m). 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 (2009h). 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 (2009i).

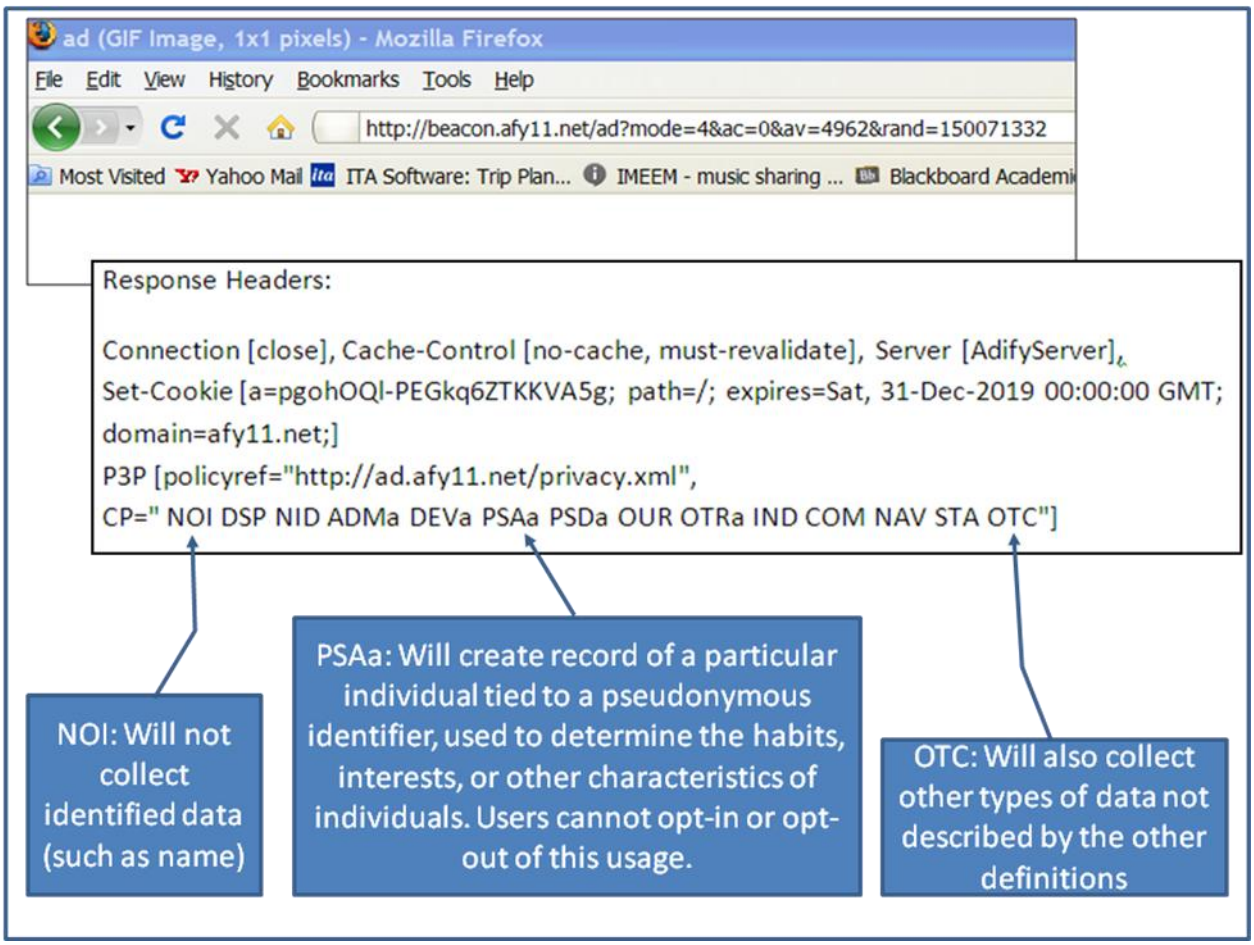

Figure 4: Analysis of data collection uses for this Web beacon.

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 (2009e). 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.

In fact, none of the companies linked to these nine Web beacons are mentioned in Levi's privacy policy. The only third party mentioned is the digital advertising provider Avenue A (2009j), but none of these Web beacons link to Avenue A.

An analysis of the data retention settings shows three of the beacons will 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 (2009h; 2009i), no such data retention information could be found for any of these companies.

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

RISKS TO TRUST IN E-COMMERCE FROM BEHAVIORAL TARGETING

The Levis brand has a long association with American values of independence and autonomy. Levi's use of behavioral targeting directly contradicts the values that serve as a foundation of customer trust in the Levis brand. The perceptions of integrity and benevolence that e-commerce sites labor to establish can be seriously damaged by behavioral targeting in its current state.

This study shows the amount of data collected and shared with third parties is much higher that what is described in the Levis privacy policy. While Levis promises to never share personal information without consent, it makes no such promise about the data collected for behavioral targeting, which it describes as anonymous data. The code displayed in Figure 2 shows multiple Web beacons being attached during a single visit. The cookie displayed in Figure 3 has a tag value that is shared with a behavioral targeting company. Levis customers are not asked to consent to these practices, and the partners that Levis shares information with are not identified. The omission of a clear explanation of behavioral targeting practices diminishes the credibility of the Levis privacy policy, which begins with this phrase: "Levi Strauss & Co. is deeply committed to maintaining your privacy," (2009f). When an e-commerce site loses credibility, it quickly loses the trust and loyalty of its customers (Gefen, Karahanna et al., 2003).

For customers who associate blue jeans with American independence and freedom, Levi's pervasive use of Web beacons and ongoing data collection with unidentified marketing partners may come as a shock. In a consumer driven market, even the appearance of deceptive practices carries a great risk, and can result in a public relations nightmare.

There can also be broader social consequences from the impact of these practices. Evidence suggests behavioral targeting was a factor during the final run up in prices before the collapse of the American housing market in 2007. The role of behavioral targeting in the aggressive marketing of sub-prime mortgages is documented in "Supplemental Statement in Support of Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Online Practices," a legal brief submitted to the FTC by the Center for Digital Democracy in November 2007 (2007). Keywords such as 'mortgage' and 'refinance' were going for as high as $20 to $30 dollars per click. Consumers shopping for sub-prime mortgages were filtered out and aggregated by search engines such as Google, Yahoo and MSN. These prospects were then sold to interested parties offering financial services (2007).

Behavioral targeting has been described by Cindy Cohn, the legal director of the Electronic Frontier Foundation, as "the surveillance business model," (Cohen, 2009). Not asking for explicit consent, and using anonymity to sanitize the tagging of individuals are components of behavioral targeting that can destroy trust in e-commerce. Even if consumers are anonymous, these advertising networks are silently collecting data to influence their purchase decisions. One motivation for privacy is to protect autonomy, and block the use of information to change power dynamics within a relationship (Waldo, Lin et al., 2007).

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.

Another concern behavioral targeting triggers is its resemblance to techniques employed by hackers and viruses. Compare the case of Levis.com planting Web beacons in their customer's browsers to the virus technique known as a Trojan horse. Like a Trojan horse, a seemingly benign file from Levis.com web site is downloaded. It then releases its payload – no less than seven Web beacons connecting the unsuspecting visitor to multiple advertising networks. For a firm like Levis, whose brand has been carefully crafted to align with American symbols of individualism and independence, its role as an enabler of widespread consumer tracking could be very damaging.

FUTURE RESEARCH

Many streams of research arise from these findings. This case study looks at a single web site. The next objective is a detailed profile by industry as to the levels of use of behavioral targeting methods.

Another important question is awareness by consumers, as to their exposure and susceptibility to behavioral targeting. This can be illuminated by a study of the level of awareness consumers have regarding these practices, and whether an increased level of awareness is related to a decrease in trust in e-commerce.

In the meantime, what can consumers do to protect their privacy? Right now there are few options. Conti suggests that abstinence or withdrawal from the online world is the only method guaranteed to work (Conti, 2009), but it is not a practical alternative. One simple and relatively effective method is to clear both cookies and temporary Internet files at the end of each browsing session. This will delete both third party cookies and the Web bugs saved in the browser cache. In order to develop other methods a research project has been planned to examine the types targeting tags obtained through Web browsing. The goal will be to discover behavior targeting tags associated with specific browsers, and develop reliable methods to block and erase those tags.

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 (2009d), 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 (2009c). At the very least, e-commerce sites should consult their customers about what type of information is being collected. They should conduct focus groups with customers, and carry out walk-throughs where these data collection methods are explained in neutral terms. The availability of opt-in and out-out mechanisms needs to be carefully considered, and probably revised to become more robust and comprehensive.

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

1. (2007). "Supplemental Statement In Support of Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Online Marketing Practices." Center for Digital Democracy. Accessed on February 15, 2009, <http://www.democraticmedia.org/files/FTCsupplemental_statement1107.pdf>.
2. (2009a). "Add N Edit Cookies Project." mozdev.org. Accessed on February 21, 2009, <http://addneditcookies.mozdev.org/>.
3. (2009b). "Atlas Solutions - Online Advertising: Advertiser and Publisher Ad Serving Solutions." Atlas Solutions. Accessed on February 21, 2009, <http://www.atlassolutions.com/index.aspx>.

4. (2009c). "FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising." Federal Trade Commission. Accessed on February 15, 2009, <http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf>.
5. (2009d). "The Future of Privacy Forum." The Future of Privacy Forum. Accessed on February 16, 2009, <http://www.futureofprivacy.org/>.
6. (2009e). "The Leader in Online Channel Management Solutions and Services | ChannelAdvisor." Channel Advisor. Accessed on February 23, 2009, <http://www.channeladvisor.com/>.
7. (2009f). "Levi Strauss & Co.'s Commitment to Privacy." Levis.com. Accessed on February 20, 2009, <http://us.levi.com/helpdesk/index.jsp?display=safety&subdisplay=privacy&clickid=botnav_privacy_img>.
8. (2009g). "Network Advertising Initiative." Network Advertising Initiative. Accessed on February 15, 2009, <http://www.networkadvertising.org/index.asp>.
9. (2009h). "P3P - The Platform for Privacy Preferences." World Wide Web Consortium. Accessed on February 21, 2009, <http://www.w3.org/P3P/>.
10. (2009i). "P3P Compact Policies." P3P Writer. Accessed on February 21, 2009, <http://www.p3pwriter.com/LRN_111.asp>.
11. (2009j). "Razorfish: The Agency for Marketing, Experience & Enterprise Design for the Digital World." Razorfish.com. Accessed on February 23, 2009, <http://www.razorfish.com/>.
12. (2009k). "The TamperData Project." mozdev.org. Accessed on February 21, 2009, <http://tamperdata.mozdev.org/>.
13. (2009l). "Tracking Macromedia Flash Movies." Adobe. Accessed on February 19, 2009, <http://www.adobe.com/resources/richmedia/tracking/>.
14. (2009m). "Vertical Ad Network Solutions by Adify." Adify. Accessed on February 21, 2009, <http://www.adify.com/>.
15. (2009n). "Web Analytics | Online Business Optimization by Omniture." Omniture. Accessed on February 21, 2009, <http://www.omniture.com/en/>.
16. Ackerman, M. (2000). "The Intellectual Challenge of CSCW: The Gap between Social Requirements and Technical Feasibility." *Human-Computer Interaction* 15(2/3): 179-203.
17. Cohen, N. (2009). "As Data Collecting Grows, Privacy Erodes." *The New York Times*, February 16, 2009.
18. Conti, G. (2009). *Googling Security*. Boston, MA, Pearson Education, Inc.
19. Dixon, P. (2007). "The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation." World Privacy Forum. Accessed on February 15, 2009, <http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf>.
20. Fukuyama, F. (1995). *The social virtues and the creation of prosperity*. New York, Free Press.
21. Gefen, D., Karahanna, E. and Straub, D. W. (2003). "Trust and TAM in Online Shopping: An Integrated Model." *MIS Quarterly* 27(1): 51-90.
22. Jackson, C., Bortz, A., Boneh, D. and Mitchell, J. C. (2006). "Protecting browser state from web privacy attacks." *Proceedings of the 15th international conference on World Wide Web*, Edinburgh, Scotland, ACM.
23. Jensen, C., Sarkar, C., Jensen, C. and Potts, C. (2007). "Tracking website data-collection and privacy practices with the iWatch web crawler." *Proceedings of the 3rd symposium on Usable privacy and security*, Pittsburgh, Pennsylvania, ACM.
24. Leggiere, P. (2009). "Targeting For Value." MediaPost Publications. Accessed on February 15, 2009, <http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=98826>.
25. Petronio, S. (2002). *Boundaries of Privacy: Dialectics of Disclosure*. Albany, State University of New York Press.
26. Solove, D. J. (2004). *The Digital Person: Technology and Privacy in the Information Age* New York, New York University Press.
27. Story, L. (2007). "FTC Member Vows Tighter Control of Online Ads." *The New York Times*, November 2, 2007.
28. Sullivan, J. (2006). *Jeans: a cultural history of an American icon*. New York, Gotham Books.
29. Waldo, J., Lin, H. S. and Millett, L. I. (2007). *Engaging Privacy and Information Technology in a Digital Age*. Washington, DC, National Academies Press.
30. Westin, A. (1967). *Privacy and Freedom*. New York, Atheneum.