Papers

Cookies: What do consumers know and what can they learn?

Received: 2nd April, 2006

Marilyn Lavin
is a Professor of Marketing at the University of Wisconsin-Whitewater where she regularly teaches internet marketing (undergraduate and MBA) and retail management. She has published in such journals as the Journal of Consumer Research, Journal of Retailing and Consumer Services, and International Journal of Retail and Distribution Management.

Abstract The present research investigates consumer knowledge about tracking cookies and considers the value of the information on those devices appearing in the privacy policies of two major websites. The study finds that the majority of the sample believed cookies are used to collect personally-identifiable information and that, as a result, many regularly reject or delete all cookies on their computers. Sample members also found that the material related to cookies in the privacy policies of the two sites increased their understanding of the consumer benefits from such tracking software.

INTRODUCTION

Among the most important advantages the internet offers marketers are the opportunities to personalise, customise, and measure customer response to their offers. Today, online sellers such as Amazon can acknowledge returning visitors to their sites by greeting them by their first names, and then, based on past activity on the site, proceed to make suggestions regarding products likely to satisfy a particular customer's needs. In addition, publisher sites like the *Wall Street Journal* mine databases of information related to site visitor behaviour to create audience segments likely to respond to specific advertising appeals. Such personalisation and customisation are, in truth, only small steps toward creating the market segments of one that some enthusiasts have claimed the internet can make possible, but they do represent important advances toward implementing and maintaining strong relationships between marketers and their customers. In addition, the ability to identify exactly which appeals are effective and which are not useful offers an unprecedented benefit to marketers.

Unfortunately, at the same time that online marketers have shown increasing willingness to accept and utilise personalisation, customisation and measurement tools, consumers have become more and more wary of cookies, and some have come to equate cookies with adware and spyware. Numerous surveys have revealed that consumers are growing increasingly concerned about their privacy, and that they believe marketers may be accumulating too much personal information about them. In the extreme, consumers even report that use of the most common tracking tools, such as cookies, may make identity theft possible.

Marilyn Lavin
Department of Marketing
University of
Wisconsin-Whitewater
Whitewater, WI 53190
USA

Tel: +1 262 472 4746
Email: lavinm@uww.edu

Consumers' increasing concern for their privacy online represents an important roadblock for marketers who wish to optimise their customers' online experiences and their promotion effectiveness. Even more troubling, survey results suggest that many consumers may not have accurate information on which to base their resistance to online tracking tools. This latter issue is the major concern of the present research effort. This paper will first review the various types of tracking devices that marketers today may employ, as well as recent studies examining the issue of consumer reaction to cookies, adware and spyware. It will then examine the attitudes of a group of consumers to these topics. Of concern in this effort will be issues such as whether or not consumers have accurate information about online tracking tools, and whether or not they recognise the advantages they obtain as a result of the use of such programs. The research will also assess whether the privacy policies on existing websites contain sufficient information about what cookies are and how they are used, and whether consumers are likely to accept cookies as a reasonable means of collecting the data necessary for personalisation and customisation efforts.

COOKIES, ADWARE AND SYPWARE

A cookie is 'a small piece of software that a Website places on a user's computer to store data about the user's activities on the site'.[1] This textbook definition suggests the limited scope of data captured by these tracking tools. Barnesandnoble.com, for example, indicates in its privacy policy that its cookies only collect information on its site and only transmit these data to the company's computers or to its third-party distributors of banner ads and newsletters. The site's privacy policy also indicates the advantages a customer gains from cookies. Those benefits include faster site navigation, tracking of items placed in the shopping cart, customised site content, and storage of shipping and credit information. In addition, the policy acknowledges that its cookies allow the company to evaluate email campaign effectiveness and to monitor the number of site visitors, pages viewed and banners served.[2]

Cookies may also track site visitors' behaviour beyond the site that places them. Google places a cookie when a user clicks on a paid keyword ad. When the user lands on the conversion page of the site that sponsored the key word, the cookie sends information about this conversion back to the Google servers. This tracking activity allows Google to obtain the information that permits keyword buyers to assess which keywords are most effective.[3] Parent companies, including Dow Jones, also track site visitors across several of their sites, while other organisations such as advertising.com, Tacoda, and 24/7 Real Media have created or utilise large networks of sites that allow tracking across all members. With more data than could be obtained from tracking on only one site, this network information allows better identification of web users' interests, and, in turn, permits the placement of advertising most likely to be of interest to those users.[4]

Although cookies that track behaviour on individual sites or across networks of sites are generally placed without the permission of the site visitor, so-called adware, which is capable of monitoring behaviour across the internet, is voluntarily accepted when the site visitor downloads free applications such as toolbars, screensavers, or shopping companions. Operators such as Claria with its 'Gain' Network or WhenU and 180 Solutions do require the user to agree to accept the software that monitors his/her online activity.[5,6] Such agreement can, however, be problematic, because, in the enthusiasm to receive the free desktop application, some site visitors — including children using a household computer — may not carefully read or understand what they are accepting. In addition, Claria does not explicitly disclose that users will receive pop-ups as a result of agreeing to installation of its software.[7] Adware providers contend that they do not use personally-identifiable information. Instead, by tracking a user's anonymous online behaviour including shopping activity or by using algorithms that consider keywords, search terms and URLs, they are able to deliver a wide range of pop-up advertising that is targeted to the user's interests. Companies that use or have used the services of adware providers include Monster.com, British Airways and Priceline.com. The highly relevant nature of the advertising can make the pop-ups highly effective; in fact, one online advertising executive suggested that 'adware can be more than twice as effective as other forms of online advertising'. Nonetheless, this same marketer noted that 'The problem is that we're not 100% comfortable with the approach'.[8]

The boundary between so-called adware and spyware is hazy (and some observers would deny one exists). Generally, however, spyware would be considered to be the most insidious type of program, and it often gains access to a computer because of security breaches in web browsers. Spyware can record such confidential information as keystrokes, passwords and site visits. It can also redirect online searches. In the extreme, the computer owner loses control of his/her machine,[9] and may require professional assistance to remove the software from the hard-drive.

RECENT STUDIES RELATED TO COOKIES

During recent years, the attitudes and actions of marketers and consumers regarding online tracking software have moved in opposite directions. On the one hand, many marketers have become interested in increasing the effectiveness of online advertising, and are, as noted above, moving from relying on cookies placed on an individual site, to accepting more sophisticated software that monitors a user's activity across the web. On the other hand, growing numbers of consumers have become more concerned about their online privacy, and are becoming more aware of and taking action to eliminate the tracking software that is being placed on their computers.[10]

The depth of consumer concern regarding risks to privacy is perhaps best reflected in the results of the 2005 Pew Internet and American Life Project study. According to this report based on a telephone survey of 2,001 adults in May–June 2005, 91 per cent of respondents indicated that they had modified their online behaviour in at least one way as a result of unwanted programs being placed on their computers. The changes included 81 per cent who had stopped opening unknown email attachments, 48 per cent who no longer visit websites they suspect of loading unwanted software, 25 per cent who no longer download files from peer-to-peer networks, and 18 per cent who have switched to another internet browser.[11]

The Pew study is only one of several recent reports that have suggested consumer concern about tracking software. In December 2004, Forrester

Research found that many computer users have anti-spyware programs and regularly remove cookies.[12] Similarly, in March 2005, Jupiter Research reported that 58 per cent of computer users deleted cookies in 2004, while as many as 39 per cent indicated that they had deleted the software as regularly as every month.[13] Both the Forrester and Jupiter studies were based on survey research. Subsequent investigation by Atlas Solutions also found that respondents reported high levels of cookie deletion, but Atlas did not rely solely on self-report information. Rather, the company also examined respondent computers. That research showed that 43 per cent of the respondents who reported deleting cookies every week had cookies that were over 45 days old, while those who stated that they deleted monthly actually got rid of cookies about every 59 days. These findings were also supported by research conducted by InsightExpress. That organisation found that only 35 per cent of persons who agreed to delete cookies actually knew how to carry out the task.[14]

A recent *eMarketer* report concluded that consumer perceptions of cookies and their functions are 'all over the map'. A study conducted by Dynamic Logic found that only 55 per cent of respondents indicated that they 'definitely know what cookies are', while a survey conducted by BurstMedia reported their research showed 21.4 per cent of US internet users claimed to know 'a lot' about cookies, 28.1 per cent had 'some information, but not a lot', 19.9 per cent had 'a little', and 30.4 per cent knew nothing.15 Two InsightExpress surveys internet users found that 79.6 per cent of those questioned claimed to know what cookies are, but that only 25 per cent of that number could accurately define a cookie or its function. The remainder of those claiming knowledge of cookies offered erroneous information including beliefs that cookies link customers to a specific site, that they permit spyware to infect computers, or that they bring up webpages that are similar to those previously visited. Such findings are very problematic because they seem related to the reasons many of the InsightExpress respondents gave for regularly deleting cookies: 57.2 per cent said they deleted cookies to remove spyware/adware, 42.9 per cent to eliminate spam, 38.7 per cent to prevent pop-ups, and 33.8 per cent to prevent viruses.[16]

STUDY PROBLEM AND METHOD

Consumers' willingness to delete cookies is of concern to marketers who wish to use such devices to tailor more effective promotion campaigns. At the same time, consumers' limited knowledge of the benefits of cookies, coupled with a Jupiter finding that 44 per cent of internet users believe that deleting or blocking cookies will enhance their security online[17] suggest the likelihood many internet users may have insufficient information about tracking software. Such ignorance may be injurious to many legitimate marketing efforts, limit customer site experience, and, most seriously, leave many internet users vulnerable to online privacy invasion.

This study seeks to contribute to the growing body of information related to consumer knowledge of cookies and to consider whether or not the information that marketers are currently providing is sufficient to change erroneous beliefs. To accomplish this purpose, the research examined the content of student posts to online discussions related to cookies that occurred during a MBA-level course on internet marketing that took place in the summer of 2005. The class discussion closely paralleled an online focus group; students were free to exchange opinions and were encouraged to consider personal experience.

The sample in this study is not representative of the general online population. Rather, it could be argued that this group should be considered more internet-savvy than the average online customer, as it was composed of persons who were sufficiently comfortable with the internet to consider taking an online course and pursue an online degree. Moreover, because the course was a graduate class, sample members all were college graduates, and consequently, had a considerably higher level of educational attainment than do most internet users. Finally, the online mode of delivery of the class permitted student registration from a broad geographic area. The 41 students were enrolled from 12 states, one was foreign exchange student from Thailand, one was with the US Army in Germany, and another was a resident of the Czech Republic.

During the class, students were required to post to online discussions related to 14 different topics and to a series of articles chosen from the *eMarketer* newsletter. For the purposes of this study, two topics were particularly pertinent: first, a discussion of an article entitled 'Tossing cookies', which appeared on 26 May, 2005 and which was discussed from 2–3 June, 2005; and secondly, a discussion based on the students' examination and comparison of the privacy policies that appear on the US-based bookselling Barnes and Noble site and on the site of the UK bookseller, WH Smith, which took place between 23–25 June. The discussion of 'Tossing cookies' occurred before the class was scheduled to read the text material containing information of customer tracking online or view the online lecture on this subject; the Barnes and Noble/WH Smith discussions took place after exposure to both of those sources of information. Although other information related to the topic of this paper was exchanged during other online class discussions, that material has not been considered in this analysis.

The data gathered in the online discussions will be treated in the present analysis in a manner similar to information gathered through online focus groups. Some number counts of persons expressing certain attitudes and expressing related opinions will be provided; however, no statistical analysis of the data will be undertaken. Instead, this qualitative effort will focus on attempting to assess the participants' knowledge of cookies and other tracking devices and to estimate the level of their concern about that software through a consideration of the statements made in the two online discussions.

FINDINGS

'Tossing cookies' discussion

In its article, 'Tossing cookies',[18] the *eMarketer* newsletter reported the results of a WebTrends study that found consumers worldwide were not just deleting cookies, but increasing their use of blocking programs that reject third-party cookies. According to WebTrends, only 2.84 per cent of site visitors rejected those types of cookies in January 2004, but 12.4 per cent blocked them in April 2005. The research data further showed that rejection of such cookies varied by industry: retailers had the highest rate of rejection at 16.9 per cent, while the legal/accounting industry had the lowest at 10.6 per cent. Telecom, health care, manufacturing, transportation, technology, media, insurance, services, and travel/hospitality had rejection rates that fell between those extremes.

Although the *eMarketer* article specifically mentioned that it was third-party cookies — those described earlier as adware that are used to track behaviour across the web to target pop-up ads and contextual advertising — that were being blocked, only two students specifically noted this fact in their discussion posts. One of those two indicated that first-party cookies — those placed by the particular site being visited — were less likely to be blocked, while the other mentioned that she frequently ordered flowers online, and 'when the cookie is placed on my computer showing I bought flowers … companies are able to see what I'm buying. Different companies that may offer floral services, can allow a pop up on my computer that highlights different floral sales or occasions to send flowers, thereby enticing me to order through their company instead of another'.

Even though they did not differentiate between third-party and first-party cookies, a number of students indicated accurate knowledge of cookies in general. For example, one wrote that they help target 'ads and tactics to a specific user', and went on to note that 'they can't identify the user, just the computer'. Another believed cookies to be 'a simple and easy way to get information that is non-intrusive'. Others considered specific benefits associated with cookies including 'access to commonly used websites', not having to sign in on a site, remembering preferences of site visitors, as well as allowing marketers to know how many times an ad was viewed by unique site visitors and 'to track what users are interested in by their clicking'. Many were also aware that they could not have full access to some websites without accepting cookies from the site, and one student reported that the only thing about cookies that he did not like was the fact they took up space on his hard drive.

Although cookies do not link web activity with personally-identifiable information, many of the discussants did not know this fact, and believed that cookies violated their privacy. Under a post titled 'Privacy Please', one student erroneously noted that deletion of cookies would cause marketers to lose an understanding of the 'customer's demographics', while another agreed and further argued that cookie rejection would lead marketers 'to find better ways to be creative to get the [demographic] information'. Still, another saw online tracking as 'personal' when she stated 'I don't like that fact that someone can see what and where I am going'; she also noted later that she had assumed that cookies tracked 'personal info'. In addition to these class members, seven others associated cookies with privacy invasion, and one even suggested that cookies are used to steal email addresses.

Aside from issues strictly related to privacy, six students argued that cookies should be 'opt-in'. One wrote: 'Websites don't own the computers their customers are using, so they have no right putting information on that machine'. Similarly, another noted: 'I hate cookies and script files … anything that is installed or loaded to my PC without my permission'.

Thirteen of the students volunteered that they either regularly rejected or deleted cookies. Several recognised that these actions prevented their access to some sites, but they did not see this as a major problem. However, the knowledge with which they approached this task was quite varied. Two students used the Firefox browser, and reported rejecting most, but not all cookies. Their discussion posts suggested that they did differentiate between sites where they wanted customisation and sites where they did not. Most students, however, simply noted deleting 'my cookie files every once in a while', or 'pretty regularly', or that the goal was to 'ensure my computer is as cookie free as possible'. Those comments appear to indicate that the students got rid of all cookies. However, a couple of those who reported deleting did see their actions as problematic. One noted 'I often run into difficulties determining which Cookies I should keep because they are identified in such a cryptic manner', while a fellow classmate expressed even greater frustration when she wrote: 'It is when the hidden cookies that are on my computer [sic] that I wish I had my own computer geek to fill me in as to what all of this is on my PC'.

Barnes and Noble/WH Smith discussion

Several weeks after discussing the 'Tossing cookies' article, the class considered the privacy policies on the US site of Barnes and Noble and the site operated by the British bookseller, WH Smith. During the time between the *eMarketer* article discussion and that related to the two websites, class lectures and the textbook considered issues such as online tracking, spyware, and attitudes toward privacy in the USA and in the EU. The purpose of the Barnes and Noble/WH Smith exercise focused on a comparison of the privacy policies on the two sites and a consideration of whether either site appeared to be violating visitors' privacy. In meeting that class requirement, a substantial number of students considered how the cookies were handled in the two privacy policies.

Students noted many similarities between the two sites. In particular, they commented on the facts that both sites placed cookies, shared with affiliates, offered 'opt-out', and monitored 'the activity of website users for research purposes'. Regarding the specific issue of cookies, a student noted that one FAQ on the WH Smith site dealt exclusively with cookies. Several also commented on the fact that Barnesandnoble.com would not allow online ordering if cookies were rejected; by contrast they found that WH Smith announced that, without cookies, the user would not be able to take full advantage of the site, but that the British company did not explicitly indicate that online ordering could not take place.

Even after reviewing text material on cookies, viewing an online class lecture on cookies and related tracking software, participating in the 'Tossing cookies' discussion, and reading the explanation of how both Barnes and Noble and WH Smith use cookies, one student remained unconvinced of their value. Her first post to the discussion noted: 'It is kind of hypocritical, don't you think. It's a privacy policy yet, they put cookies on your computer to track your use. I know they do not know your identity, but I felt it was rather ironic.' She further commented 'Why should I be limited to what I see on Smith's site simply because I do not except [sic] their cookies?' Her posting suggests the difficulty that marketers may have in educating some consumers. After exposure to more information than the average consumer is likely to encounter, she did recognise that a site's cookies would not identify her personally; on the other hand, she did still did not recognise that her rejection of cookies necessarily limited the customised content the site could offer. Another student, however, responded 'I see your point about privacy and cookies being ironic. However, I have gone thru [sic] a transformation of sorts when it comes to Cookies. I recognise that some cookies are good because they actually serve a useful purpose (ie storing and retrieving information, providing me content before I ask for it, etc).'

Several class members believed that the two sites educated consumers about cookies in an appropriate manner. One wrote: 'If I had no previous knowledge of cookies this [the information contained in the two privacy policies] would have been a good explanation. The websites also make sure to inform the consumer that cookies help your overall internet experience. I think if we had this module before the module on cookies I would have been less critical of cookies.' Similarly, another commented: 'I like how BN presented the info on cookies. It explained what they were, why they use them, how they use them, and the benefit to the customer.' And a third noted: 'The B&N site … had a simple explanation of how cookies work, and why they are not all bad. They even went so far as to admit most people don't know cookies are being placed on their computers.'

IMPLICATIONS

The findings from this research suggest the level of misconception about cookies that exists among many internet users — including those likely to be highly informed. Although the article used to generate the first discussion was concerned with third-party cookie rejection, very few class members differentiated between those tracking devices and the first-party cookies placed by a site being visited. Moreover, before participating in the online discussion and reading text material, many of the students believed that cookies collected personally identifiable-information, and, consequently, the devices were seen to violate consumer privacy. Despite such serious misconceptions of what cookies actually do, however, many of the online class members indicated that they regularly blocked or rejected cookies — although some admitted that by so doing they often eliminated cookies that benefited them as well as those they believed were nuisances.

The results of this study — especially willingness to reject or delete cookies — are in keeping with earlier research studies. Whether negative attitudes toward cookies can be changed is, however, a topic of debate. Richard Stiennon, Vice President of Research at Webroot Software Inc — the producer of the popular antisypware program, Spy Sweeper, believes that 'Most end users mistrust cookies', and will not 'distinguish between good and bad cookies'.[19] *eMarketer* Senior Analyst, David Hallerman does not share this attitude. Hallerman believes that marketers have the responsibility to persuade consumers to accept cookies. In fact, he argues that a full-blown 'cookie campaign' aimed at the half of all internet users who are wary of cookies would be appropriate. He contends that such users can and should be convinced of the benefits associated with personalisation, easy shopping and site navigation, and of exposure to relevant advertising.[20]

The findings of the present research suggest the likelihood that consumers might indeed be open to a campaign such as that suggested by Hallerman. Although some students were aware of the function of cookies before taking the class, a large number, before being exposed to the course materials, saw cookies as means of gathering personal information, email addresses, and invading privacy. Such erroneous information undoubtedly played a major role in their decisions to reject and delete all cookies. The information currently available on websites about cookies, however, seemed to allay their fears. When considering the description of cookies and their use that is available on the Barnes and Noble and WH

Smith sites, the students found the information forthright and easy to understand. In fact, one even acknowledged that if he had not known what cookies were, 'this would have been a good explanation'.

Although the students found the information on cookies helpful and complete, they were unhappy about the difficulty they experienced when seeking out the privacy policies on both sites. Many commented on the fact that Barnes and Noble had only a tiny, hardly visible, link at the bottom of its homepage, while most needed the explicit instructions provided in course materials to find the policy on WH Smith. Several noted they believed the policies should have greater visibility.

Many of the students mentioned that they had never before read a privacy policy before and would not have done so had there not been a class assignment. They seemed surprised that the information they found in the sites' disclosures did, in fact, increase their understanding of cookies, and, in most cases, increase their acceptance of these tracking programs. This finding suggests that a campaign to educate consumers about cookies can be effective, and that marketers should consider heightening awareness of the information they provide on their sites.

CONCLUSION

The current findings come from students with an above average comfort level with the internet and above average educational attainments. Consequently, the results of this study cannot be generalised to the entire online population. Nonetheless, marketers should be concerned that even among the most internet-savvy consumers, misconceptions about cookies appear to be widespread. They should also be cognisant of the fact that such customers can be educated about the true benefits that cookies can provide.

To date, most marketers have confined their 'cookie education' to a section of their site's privacy policy, which is often hidden on the site. The information contained in the policies with regard to cookies is valuable. The vast majority of consumers would most likely be able to understand its content. Most site visitors, however, do not read privacy policies. This fact suggests that marketers must become more involved with such educational efforts. They need make certain that consumers truly understand the purpose of cookies, and the benefits to the site visitor associated with such devices. If marketers do not take this initiative, the percentage of the online population that regularly rejects or deletes cookies will continue to grow, and site owners will lose important opportunities to customise, personalise, and assess the effectiveness of their promotion efforts.

References

1 Roberts, M. L. (2003) 'Internet Marketing: Integrating Online and Offline Strategies'. McGraw Hill, New York.

2 Barnesandnoble.com. Privacy policy reviewed 7 September 2005, www.barnesandnoble.com/help/cds2.asp?PID=8104&z=y, accessed 7 September, 2005.

3 Google. Conversion tracking demo and FAQs, services.google.com/tutorial/cvt/cvt.html, accessed 7 September, 2005.

4 Williamson, D. A. 'What comes before search?' *eMarketer* white paper, www.emarketer.com/Reports/Whitepaper.aspx?behavior_white_sep04, accessed 20 September 2004.

5 Claria.com. (2005), www.claria.com/privacy/policies/, accessed 9 September, 2005.

6 WhenU.com, www.whenu.com/pc_privacy_policy.html, accessed 10 September, 2005.

7 Edelman, B. (2004) 'What Claria doesn't disclose (any more)'. Available at: http://www.benedelman.org/news/111505-1.html.

8 Totty, M. (2004) 'Pesky pop-up ads go mainstream', *Wall Street Journal*, 22 June, B1.

9 O'Brien, T. L. and Hansell, S. (2004) 'Barbarians at the digital gate', *New York Times*, 19 September; 3.1.

10 *eMarketer* (2005) 'The confusion over cookies',

eMarketer, 19 July. Available at: http://www.emarketer.com/Report.aspx?cookies_aug05.

11 Fox, S. (2005) 'Spyware'. Washington, DC: Pew Internet and American Life Project, 6 July. Available at: http://www.pewinternet.org/pdfs/PIP_Spyware_Report_July_05.pdf.

12 Chatham, B. (2004) 'Web users toss their cookies'. Available at: http://www.forrester.com/Research/Document/Excerpt/0,7211,35957,00.html.

13 Jupiter Research (2005) 'Accurate website visitor measurement crippled by cookie blocking and deletion'. Press Release, 14 March. Available at: http://www.jupitermedia.com/corporate/releases/05.03.14-newjupresearch.html.

14 Smith, L. (2005) 'Consumers' misunderstanding of cookies; research from Insight Express', 26 April. Available at: http://www.safecount.org/docs/Cookie_Research_Final.ppt#510,1,Slide%201.

15 *eMarketer*, ref. 10 above.

16 Smith, ref. 14 above.

17 Jupiter Research, ref. 13 above.

18 *eMarketer* (2005) 'Tossing cookies', *eMarketer*, 26 May. Available at: http://www.emarketer.com/SiteSearch.aspx?arg=tossing+cookies [subscription only].

19 Kesmodel, D. (2005) 'Marketers seek to make cookies more palatable', *Wall Street Journal*, 17 June, B1.

20 *eMarketer*, ref. 10 above.