BEWARE OF ADWARE: INTERNET USER AWARENESS, 
PERCEPTIONS AND CONSEQUENCES

Penny M. Simpson, University of Texas-Pan American, pmsimpson@panam.edu
Claude L. Simpson, Jr., University of Texas-Pan American, csimpson@panam.edu

ABSTRACT

Internet marketers increasingly engage in activities that allow them to better track and understand consumer online browsing and purchase behavior for targeting and personalization purposes. Users of Internet services may consider such practices unethical and a violation of privacy and respond in ways that may ultimately harm company efforts. The purpose of this research is to determine consumer awareness and perceptions of two such activities, cookies and adware, and consumer response to the practices.

Keywords: Internet privacy, computer security, spyware, adware, online tracking

INTRODUCTION

The Internet and its accompanying computing power has been a boon to marketers looking for ways to better identify and understand prospective customers. For example, marketers are able to track and view Internet browsing habits and purchases and use the information to target likely customers. Potential problems may arise, however, when overzealous marketers use this capability unethically or without consumer knowledge. When customers discover these practices, they may react in a number of ways, such as by boycotting the companies involved, by purchasing blocking software or even by suing the companies or by lobbying for restricting legislation. Each of these reactions may be harmful to companies involved.

The purpose of this research is to examine Internet users’ ethical and other perceptions about computer privacy and the ability of companies to access and retrieve information on privately owned computers. We also explore consumer awareness of two practices employed by Internet marketers, cookies and adware, and the likely consequences of detection of such practices. The next section begins with background research on computer privacy and consumer response to privacy concerns and unethical marketing practices in general. We then detail the methodology used in this research, present the data analysis results, and draw conclusions for Internet marketers.

COMPUTER PRIVACY AND CONSUMER RESPONSE TO PERCEIVED UNETHICAL PRACTICES

Cookies and Adware are two types of Internet capabilities that marketers use to track the purchase patterns of Internet browsers. The first, cookies, are text files placed on hard drives by an advertiser or Web server. These files contain information about Web sites visited, usernames and passwords (1). Cookies have been used for years now and most computer users seem to be aware of their existence and Internet browsers commonly contain a feature that will allow users...
to adjust the computer system security to opt in or out of cookies placements. A much newer practice is Adware. Adware is defined as “commercial software used for several purposes. It may record the Web sites a user visits or online ads that a user clicks. This information is sent to the ad company’s servers and combined with that of thousands of other users to form aggregate information” (8). Adware is usually installed on a consumer’s computer when shareware or freeware is downloaded and the computer owner may not be aware of the installation.

Both cookies and adware invade an Internet browser’s computer and install files for the benefit of the marketer. This practice of placing unwanted files on personal computers without permission may be considered an invasion of privacy and unethical by many computer users. Most consumers have expressed concern about computer privacy and the security of private information since the advent of the Internet. In fact, one recent survey found that about 75 percent of consumers are concerned that companies provide confidential customer information to others without permission and almost as many consumers believe that their transactions on the Internet are not secure (10). Yet another study found that 54 percent of the consumers surveyed online felt that customer information was not handled in a ‘proper’ or confidential manner and that current laws are not sufficiently protective of consumer privacy (5).

These consumers’ perceptions of privacy and security violations by Internet marketers have the potential for significantly negative effects, depending on behavioral reactions of consumers to such practices. The few marketing studies that have examined the impact of perceived unethical company activities on consumer responses have found significant effects. For example, Simpson, Brown and Widing (7) found strong effects of detected subliminal embeds in advertisements on consumer response to the ad, including purchase intention, Thomas, Vitell, Gilbert and Rose (9) found a negative effect of consumer perceived unethical cues in a retail store on satisfaction with the store, and Folkes and Kamins (2) found that perceived unethical activities of a firm (negative hiring practices) negatively influenced consumer attitudes toward the firm in general.

Computer privacy violations may be viewed by consumers as unethical and may have significant negative effects on infringing companies, though different consumers may respond in different ways. Though no known academic studies have examined this possibility, some practitioner surveys point to the potential. One study found that only 26 percent of households in the U.S. have trust in their Internet activities and 43 percent believe that businesses have little reason to guard consumer privacy (3). The result likely affects firm profits as one study found that retailers lost $6.2 billion in sales from consumer privacy concerns (4). Nevertheless, evidence from Sheehan (6) suggests most online consumers are pragmatic about privacy, accepting privacy violations under specified conditions, but that age and education level affect concern for privacy.

Taken together, evidence from prior research and logic suggests that the use of cookies and adware, which may be perceived as violating privacy or as unethical, will likely evoke consumer reaction, if detected. Though consumer reactions will vary, the impact to Internet marketers may be very significant; yet, no known prior studies have examined the relationship.
METHODOLOGY

The study was conducted in two parts. In part I, a questionnaire designed to determine student Internet users’ perceptions and awareness of adware, cookies, computer privacy, and information security was developed and administered to 121 volunteering students at a Southern, predominately Hispanic university during class. Respondents were first asked to indicate whether they owned a personal computer and how many hours each week they spent on the Internet. Then respondents were asked to rate their agreement with specific, single-item statements about awareness and importance of privacy and security, online tracking, and receiving online ads using a seven-point Likert scale, with a ‘1’ indicating strongly disagree and a ‘7’ meaning indicating strongly agree. Because the purpose of this research was descriptive—to assess current attitudes and behavior toward privacy infringing practices—only single-time questions were deemed needed. Awareness of cookies and adware was determined by asking respondents to define the terms. The final question in part I asked respondents to tell “what would you do if you discovered that a company had installed a software program on your computer that could send information contained on your computer back to the company.”

After completing Part I of the questionnaire, respondents were given Part II, which defined the terms cookies and adware and asked students to download and run free software that scans and detects such files on their personal computers before answering the questions. If the respondent found these types of files on their personal computers, they were asked to tell how many cookies and adware files they found, how finding such files made them feel and how they would like to respond about the finding.

ANALYSIS AND RESULTS

A total of 121 Part I and 73 Part II questionnaires were returned from the respondents. Most of the respondents (94.2 percent) had a personal home computer and spent from 0 hours to 50 hours, with a mean of 11.75 hours on the Internet each week. Respondents ranged from 19 to 43 years of age, with an average age of 23.6 years, and were mostly either computer information majors (43.8 percent) or business majors (35.5 percent), though 14.1 percent were ‘other’ majors and 6.6 were math/computer science majors.

The first section of the questionnaire asked respondents to indicate their agreement to nine specific items related to computer privacy, security and Internet marketing practices. Ratings of 1 and 2 were collapsed into the ‘disagree’ category and ratings of 6 and 7 were combined to indicate ‘agree’ with the statements and are shown below in Table I. No further analysis on the items was needed since all attitudes and behaviors used in the study were assessed using single-item measures for descriptive purposes only. Results from Table I suggest that respondents strongly valued computer privacy but are unsure about how the security or privacy of information on their personal computers, though most respondents tended to believe that no unknown programs resided on their own computers. Almost half of the respondents agreed that they ‘always’ get advertisements on their computers and most are bothered by the practice. Apparently, most respondents did not realize that Internet marketers may track browsing or purchase patterns of online consumers. Considering that these respondents value their privacy
and many are unaware of tracking activities of Internet marketers, an important question becomes how would they react and respond to potentially invasive practices such as cookies and adware.

### TABLE I

<table>
<thead>
<tr>
<th>Question</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer privacy is very important to me.</td>
<td>0.8</td>
<td>3.3</td>
<td>85.9</td>
</tr>
<tr>
<td>Information on my home computer is very secure.</td>
<td>14.0</td>
<td>28.1</td>
<td>27.3</td>
</tr>
<tr>
<td>No person or company is able to access the information on my personal home computer.</td>
<td>29.7</td>
<td>19.8</td>
<td>21.5</td>
</tr>
<tr>
<td>The only programs on my personal home computer are the ones I have installed or had others install.</td>
<td>14.1</td>
<td>12.5</td>
<td>54.2</td>
</tr>
<tr>
<td>I am always getting pop-up and banner advertisements on my personal home computer.</td>
<td>19.0</td>
<td>9.9</td>
<td>47.1</td>
</tr>
<tr>
<td>Some Internet companies often track my visits to different Web sites.</td>
<td>9.2</td>
<td>24.4</td>
<td>38.6</td>
</tr>
<tr>
<td>Getting ads on my home computer doesn't generally bother me.</td>
<td>69.4</td>
<td>11.6</td>
<td>9.1</td>
</tr>
<tr>
<td>One company cannot know what products I buy from other companies on the Internet.</td>
<td>45.4</td>
<td>25.6</td>
<td>10.8</td>
</tr>
<tr>
<td>Some companies 'watch' where I go and what I buy when I am on the Internet.</td>
<td>10.8</td>
<td>27.5</td>
<td>40.0</td>
</tr>
</tbody>
</table>

Source: Questionnaires

This question is addressed by having students first define the terms ‘cookies’ and ‘adware’ to determine awareness, and then by answering an open-ended question about their likely response. One of the authors read the definitions of terms supplied by respondents and their likely responses to the Internet marketing practices for coding and analysis purposes. Definitions were coded as either ‘understand’ or ‘don’t understand’ the term and responses were coded into a number of categories such as ‘remove the program,’ ‘contact the company,’ ‘upset, disturbed or angry by privacy violation,’ and ‘sue, spam, fine, or hurt the company.’

Most of the respondents (65.2 percent) could correctly and completely define the term ‘cookies,’ however, only 24.4 percent seem to truly understand the meaning of ‘adware.’ Respondents cited a number of likely responses, both attitudinal and behavioral, in reaction to discovery of adware type programs on their computers. By far, the most often mentioned response was to remove or uninstall the programs (33.53 percent) followed by being disturbed, upset or angry or violated (23.12 percent), the desire to sue or harm the offending company (10.98 percent) or contact the company (10.4 percent). About 10.4 percent of the respondents indicated that they would install or use blocking software or a firewall.

Part II of the questionnaire asked respondents to run a free version of a downloadable application such as Spybot or Spyhunter to determine the number of cookies, adware, or other unknown
applications on the user’s personal computer. A total of 73 respondents returned this part of the questionnaire and 69 reported finding anywhere from 0 to 323 cookies, with an average of 52.18 cookies. An average of 24.5 adware type applications were reportedly found by 68 respondents with the numbers ranging from 0 to 349. Admittedly, many of these respondents may not have been able to determine whether the application noted was actually adware or some other type of unknown applications as the Spyhunter and Sypbot programs do not specifically state type of program found, just the severity level of the application.

Finally, respondents were asked to indicate how they felt about finding cookies and adware on their home computer systems and their intended response. All responses indicated by each informant were counted and results are reported based on the total count of responses rather than on number of respondents answering the question. Most responses related feelings of being disturbed, shocked or violated at finding cookies and adware on their personal computers (64.7 percent). An equal number of respondents indicated that they now don’t trust the Internet (6.9 percent) as indicated that they were not bothered by the cookies and adware (6.9 percent). Other responses noted by a few respondents included that presence of these applications explains why their computers run slow, that they were not surprised by the findings or that they had firewalls installed or other protective software.

Study informants mentioned a number of ways in which they intended to respond to finding unwanted cookies and adware. The most commonly mentioned responses included removing or uninstalling the offending applications (35.2 percent) and buying or running software to block such installations (31.9 percent). Other responses included that these violating companies should be sued, spammed, fined, or hurt in some way (6.59 percent), that the situation should be changed (5.49 percent), or that these privacy violators should be reported to some agency (5.49 percent). A summary comparison of the top responses to cookies and adware placed on personal computers before detection of such applications and after detection are shown in Table II.

<table>
<thead>
<tr>
<th>Feeling or Response</th>
<th>Before Detection</th>
<th>After Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove or uninstall application</td>
<td>33.5</td>
<td>35.2</td>
</tr>
<tr>
<td>Disturbed, violated or shocked</td>
<td>23.1</td>
<td>64.4</td>
</tr>
<tr>
<td>Sue, spam, fine, or harm the offending company</td>
<td>11.0</td>
<td>6.6</td>
</tr>
<tr>
<td>Contact the company</td>
<td>10.4</td>
<td>0.00</td>
</tr>
<tr>
<td>Buy or use blocking, scanning software</td>
<td>10.4</td>
<td>31.9</td>
</tr>
<tr>
<td>Do nothing/not much I can do</td>
<td>1.3</td>
<td>7.7</td>
</tr>
<tr>
<td>Report to some authority/want change</td>
<td>1.2</td>
<td>11.0</td>
</tr>
</tbody>
</table>

The table reveals that after most respondents discovered cookies and adware on their personal computers they were more likely to feel disturbed, shocked or violated and to install or run more
frequently blocking or scanning software than before detection. A few more respondents were also more likely to indicate that the situation should change or that some authority, such as a governmental agency, should be notified or feel that nothing could be done about the situation. Prior to detection of the applications, respondents were slightly more likely to want to strike out to hurt or at least contact the company because of their concern.

CONCLUSIONS

Internet consumers may react in a number of ways to Internet marketers’ perceived practices of privacy violations, such as placing cookies and adware on consumers’ personal computers to better monitor online consumer behavior. The reactions may include anything from lobbying legislators, to suing offending companies, to eliminating online activities, to simply doing nothing. Some of these potential responses may seriously impact online firms using the invasive practices; yet, little is known about consumer perceptions of the practices. This research was designed as an initial exploration into the awareness and perceptions of Internet users toward two Internet marketing invasive practices, cookies and adware.

The study found that our Internet savvy user respondents were, for the most part, aware of cookies but not of adware, highly valued their online privacy, tended to believe or did not know (neutral responses) that companies could track their online activities; but, that their own personal computers were secure in that information from the computers was probably not accessible and that no unknown programs were resident on their personal computers. When asked how respondents would react, hypothetically, to cookies and adware on their own personal computers, the most commonly mentioned response was to remove or uninstall the offending files, while almost one-fourth (23.1 percent) expressed feeling disturbed, shocked or violated by such Internet marketing practices. Other respondents mentioned that they would respond by suing, fining, spamming or harming the company in some way, some would contact the company while others would buy or use appropriate blocking and scanning software.

To convert the ‘hypothetical’ situation of reactions to cookies and adware on personal computers to a more realistic one, respondents were invited to scan their personal computers with free, adware type detection software to discover any presences of unknown files or programs. Most respondents did detect such software and reacted somewhat differently than in the hypothetical situation. About the same number of respondents would remove the unwanted applications and files in both situations, but after detection more respondents were much more likely to express feelings of violation and shock and were much more likely to purchase appropriate blocking or scanning software. They were less likely to want to sue/harm the offending company or contact the company but more likely to want the situation to change, perhaps by reporting it to appropriate authorities. Surprisingly, more respondents indicated that they would do nothing or that there was not much they could do, after detection of cookies and adware on personal computers.

Findings from this research suggest that detection of unwanted files and programs on personal computers evokes feelings of privacy violation among our Internet user respondents and they are likely to react in some way to remove such files or restrict access of their personal computers to
outside parties. Especially harmful to companies using these tracking or monitoring practices may be the possibility that consumer detection of the privacy invasions may translate to ill will toward the company and avoidance of its products. Research in this regard is unknown but bears further study.

REFERENCES