The Future Of Online Internet Marketing: A Solution To Behavioral Marketing Using Biometrics

William Gilmore, University of Houston-Clear Lake
S. Altan Erdem, (Email: aerdem@gmail.com), University of Houston-Clear Lake

ABSTRACT

Internet marketing is still an experimental area that continues to grow, evolve and adapt. With the virtual limitlessness space of the WWW, the strategic placement of internet advertisements is much more complex and goes beyond the traditional marketing approach of researching demographics. Several attempts have been made through the fields of technology and marketing to overcome the anonymousness of the computer user's interests and preferences to move toward a direct behavioral approach to online marketing; more specifically, identifying the users on the internet, collecting profiles of their interests and delivering advertisements that appeal to their specific preferences. This paper reviews the current approaches to Internet behavioral marketing and its shortcomings as well as biometrics and its potential for more effective Internet marketing.

INTRODUCTION

Currently, any amount of time an Internet user spends on the Internet will inevitably result in being prompted to create a username and password. Whether the user is a consumer purchasing an item from *e-bay* or casually viewing pictures sent from a friend through *snapfish.com*, the Internet site(s) will prompt the user to create a unique login identification and password. From a marketing standpoint, usernames and passwords, in addition to other tracking devices such as cookies, smart cards, tokens, credit cards and digital certificates are useful approaches for gathering information concerning general tastes and preferences from the general public; however, there are limitations to this technology concerning online marketing.

The market for technology used to track and capture individuals' interests in order to market to their tastes, often referred to as behaviorally targeted advertising, is growing. According to the market research firm eMarketer, it is expected that $2.1 billion will be spent on behaviorally targeted advertising in 2008 (Holahan 2006). Internet marketing in particular is evolving into more personalized advertisement approaches for strategic placements of advertisements to appeal to users' preferences. However, as Internet marketing strategies move toward a more refined and personalized marketing approach, a better method of gathering user specific information is needed. One such method that has the potential to both eliminate the frustration of usernames/passwords for users and give marketers a better picture of user's tastes and preferences is the biometric identification hardware/software.

The purpose of this paper is to review the current Internet marketing approaches of gathering data, including their pros and cons. Secondly, examine biometrics in its potential for gathering information to help marketers determine their audience better at an individual user level. Finally, review the current market for biometric technology and gain an understanding of where biometric technology for personal computers stands at the moment, and highlight some of the challenges that lie ahead.

TRADITIONAL INTERNET TRACKING

Cookies are currently one of the most common attempts to track user's activity. They gather information on the specific behavior of users by tracking the user's mouse clicks and are generally hidden to the user. They are

used to record and develop a profile of visitors' online habits for commercial solicitations (Furger 2000). These profiles help advertisers deliver personally directed advertisements that appeal to the individual tastes of the consumer and help them tailor the ads to specific users (Holahan 2006). The objective is the effective placement of advertisements to attract consumers to products for which they have a strong potential to purchase. However, this form of Internet tracking has several shortcomings. First of all, cookies identify the computer but not necessarily the user (Mitt 2000). Since several users may access the same computer, Internet site owners may obtain only those mouse clicks specific to a computer, not to a specific user. With the indefinite accessibility of public computers with internet access available in libraries, schools and other public venues, the information received from cookies can only yield a generally broad measurement of likes and dislikes as opposed to information specific to an individual. Additionally, some users may delete cookies from their computers or they may set their Internet browser to block some or all cookies. These reasons decrease the accuracy of data received from cookies and limit the ability to market to users' individual tastes and preferences.

Usernames and passwords constitute another common method currently used to identify the users of websites and capture their activities. Unlike cookies, usernames and passwords are not hidden. They are created by the Internet user and held by their knowledge or possession. They are more effective than cookies in identifying the user on a computer in addition to tracking that particular user's activities every time he/she logs in. Therefore, usernames and passwords are more effective in identifying a specific user's activity on a particular website and developing a profile. On the other hand, having to keep track of multiple username and passwords for an indefinite number of websites, in addition to keeping them both accessible and private, can be rather frustrating for the user. Also, since usernames and passwords can be passed to others, this can create discrepancies in the data gathered by marketers. Like cookies, there is a possibility of tracking the shared activity of several individuals that are using the same username and password by happenstance instead of tracking the owner.

Other forms of security measures such as smart cards, tokens, credit cards and digital certificates require physical possession and have the same drawbacks as cookies and usernames/passwords since someone other than the actual owner may be tracked. Additionally, credit cards and digital certificates are used during a transaction which limits the ability to link specific website activity to a particular consumer until the transaction is actually performed (Pons 2006). Again, these increase the uncertainty of identifying the computer user and his/her tastes and preferences for marketing purposes.

Tracking cookies, usernames/passwords, smart cards, tokens, credit cards and digital certificates are all useful for marketing purposes. However they all fall short in their abilities to track specific user's individual tastes and preferences for individual target marketing. There is still some room for improvement to positively identify the user on the computer and making this process easy for the consumer.

BIOMETRICS

The term biometrics derives its name from the Greek word "bios" (life) and "metron" (measure) (Koltzsch 2007). As stated by Corcoran (1999), biometrics is used to measure something unique about individuals and later using those unique clues to identify them. More specifically, for this article, the term biometrics refers to the use of electronic hardware/software to verify the identity of a person by using human characteristics. Some of the common methods currently used include facial recognition, fingerprint pattern recognition, iris recognition, voice recognition and signature recognition (Albrecht 2003). Currently, the main devices that are gaining attention in the market and becoming more available to businesses and individuals are fingerprint readers. Since this is the most common form found on the commercial market, the focus of this article is on fingerprint recognition.

A typical fingerprint recognition device currently available to the general public is similar to a mouse and connects to a personal computer generally via a USB port. An example of such a device is DigitalPersona's *U.are.U 4000 Reader.* This device is smaller than a deck of cards and has an oval plastic window where a user places his/her finger (Alpert 2004). The device then uses a sophisticated matching technology. Mark Alpert of *Scientific American* magazine explains:

Using a variety of complex algorithms, the DigitalPersona software determines the coordinates of up to 70 minutiae points and packages the data in a 300-byte template. The system compares these templates to match fingerprints; the fingerprint images themselves are erased to prevent any possibility of theft (Alpert 2004, p. 108).

For a consumer, the advantages of using biometric technology for identification are numerous. First, biometric technology is much more secure than common methods such as PIN numbers, passwords or security codes that are based on knowledge or possession. While these can be lost or stolen, biometric recognition relies on unchangeable characteristics instead of knowledge and it cannot be lost or stolen (Koltzsch 2007). Secondly, biometric identification is more convenient and it is always accessible. After all, one does not have to remember to "carry" biometric identification. It is simply a part of the user. Finally, biometric characteristics are rather difficult to forge or replicate. Even though there are ways to duplicate these characteristics, they are not only very difficult but also very costly. Considering these advantages, it is obvious how using biometric technology can be more effective and efficient for Internet users as well as online service providers.

What Is The Current Market For Biometrics?

The growing number of identity theft and online fraud cases are forcing financial institutions, governments and other organizations to strengthen their Internet security (Sullivan 2006). On October 12, 2005, the Federal Financial Institutions Examination Council (FFIEC) released updated guidance on the risks and risk management controls needed to authenticate customers accessing Internet-based financial services. Their guidance states that single-factor authentication (username/password) as the only control factor is inadequate for identification purposes for transactions involving access to customer information and the movement of funds. They state that "financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks" (Authentication in an Internet Banking Environment 2005). Biometric identification technology is stated in the guidance provided by the FFIEC as a control to strengthen online authentication. This indicates that there is already a potential demand for biometric technology for security purposes.

According to Scott Moody, chairman of AuthenTec Inc., the largest maker of chips for reading fingerprints, the use of biometrics in various applications is simply overwhelming (Bulkeley 2006). It is estimated that about 9% of all laptop computers shipped in 2007 will have fingerprint readers to secure and simplify remote log-ons (Bulkeley 2006). Internationally, the biometric market is already established in places such as Europe and South America. In the United Kingdom for example, all new UK passports include biometric identification beginning in 2007 (Turle 2007). It is stated that most European Union nations include a biometric fingerprint on their national drivers' licenses. As Europe and other countries move through the developments of biometric technology, this will inevitably result in the United States being more open to this technology. With the heightened security from the September 11th attacks, acceptance of biometrics in the US market has a great potential. With strong congressional interest, press coverage and public attention, biometrics has emerged as an item of interest in public and private sectors of the market including financial services and health care (Concerns Spur Biometrics Growth 2001).

At the same time, the demand for personalized marketing is growing. As mentioned earlier, according to eMarketer, $1.5 billion will be spent in 2007 for behaviorally targeted advertisements and is expected to grow to more than $2 billion in 2008 (Tynan 2007). The movement toward personalized advertisements gives marketers a new view of their audience rather than traditional marketing demographics (Klaassen 2007). As financial institutions seek stronger security measures for online transactions and as marketing firms seek more specific data on users for marketing purposes, biometric recognition potentially gives online companies the edge they need to provide security and help them identify their users' preferences for personalized marketing.

Where Is Biometric Technology Right Now?

Biometric technology is still in the opening stages of commercial development. Currently, the fingerprint readers (for eg., Microsoft's fingerprint reader) are marketed as convenience tools to identify a user logging into a personal computer or to store usernames/passwords for logging into a website. That is, they are used for convenience rather than security reasons (McMillan 2006). Several advances have been made to improve the effectiveness of the fingerprint reader devices such as matching fingerprints successfully even if a finger is placed in a different angle than the one when it was originally scanned, or if the fingerprint used is smudgy (Alpert 2004).

However, advances in fingerprint readers are still needed. For example, the *U.are.U 4000* sensor has a design goal of 1 in 50,000 chance of accepting the wrong fingerprint and a 1 in 100 chance of rejecting the correct fingerprint (Alpert 2004). While these are significant developments, continuous improvements are needed. After all, a password that consists of 6 letters or digits that contains numbers (10 different numbers) and letters (26 letters), means that the probability of someone guessing the right combination is 1 in 2,176,782,336. Obviously, there is a greater chance of the fingerprint reader accepting the wrong fingerprint than someone finding out the right password.

Also, with the emergence of new technologies, there are new crimes that develop and evolve to circumvent the controls that protect the consumer. Unfortunately, some crimes can become very violent and gruesome. For example, in March of 2005, a story from the United Kingdom's BBC reported that some car thieves in Malaysia, armed with machetes, chopped off the finger of the owner of a Mercedes S-class that was protected with a fingerprint recognition system. They did this after they were unable to bypass the immobilizer that required the owner's fingerprint. Although this case is extreme, this illustrates a challenge to owners of fingerprint recognition devices. As with all new technologies, companies will need to consider crimes such as this one when developing this new technology.

Additionally, in the US, the acceptance of biometric technology is growing, as is the demand. The stage is set for information technology experts to integrate biometrics into their websites to give marketers the edge to collect relevant data on Internet users and market to those users' specific tastes and preferences. Even though this paper was specifically focused on one of the biometric recognition characteristics, the authors recognize the fact that the entire spectrum of the biometrics deserve an in-depth look in terms of its applications in various parts and aspects of online practices. It is hoped that the exploratory studies such as this one would provide the researchers with added incentives to conduct further investigations. After all, one needs to accept that fact that while the online marketing strategy is a popular one, it is still far from perfect…

REFERENCES

1. Albrecht, A., M. Behrens, T. Mansfield, W. McMeechan, M. Rejman-Greene, M. Savastano, P. Statham, C. Schmidt, B. Schouten, M. Walsh (2003), *BIOVISION: Roadmap to Successful Deployments from the User and System Integrator Perspective*, D2.6 / Issue 1.1.
2. Alpert, Mark (2004), Security at Your Fingertips, *Scientific America*, 290 (6), 108-110.
3. Authentication in an Internet Banking Environment, www.ffiec.gov, October 12, 2005, http://www.ffiec.gov/ffiecinfobase/resources/info_sec/2006/ots-ceo-ltr-228.pdf.
4. Bulkeley, William M. (2006), How Biometric Security Is Far From Foolproof; Systems' Holes Spur Efforts To Improve Limitations; The Bummy Bear Deception, *Wall Street Journal*, December 21, B.3.
5. Concerns Spur Biometrics Growth, *Security: For Buyers of Products, Systems & Services*, December 2001, 38 (12), 7.
6. Corcoran, David, David Sims, Bob Hillhouse (1999), Smart Cards and Biometrics: The Cool Way To Make Secure Transactions, *Linux Journal*, 59 (7).
7. Furger, Roberta (2000), Who's Watching You on the Web? *PC World*, 18 (3), 33-34.
8. Holahan, Catherine (2006), Taking AIM at Targeted Advertising, *Business Week Online*, 26.
9. Jones, Mitt (2000), Web Privacy: How the Cookie Crumbles, *PC World*, 18 (3), 49.
10. Klaassen, Abbey (2007), Behavioral Targeting: The New Killer App for Research, *Advertising Age*, 78 (4), 17.
11. Koltzsch, Gregor (2007), Biometrics – Market Segments and Applications, *Journal of Business Economics and Management*, 8 (2), 119-122.
12. Krebsbach, Karen (2004), Biometrics Takes Hold Overseas, But Not in U.S., *U.S. Banker*, 114 (1), 17-18.
13. McMillan, Robert (2006), Researcher Hacks Microsoft Fingerprint Reader, *PC World Online*, (March 6).
14. Pons, Alexander (2006), Biometric Marketing: Targeting the Online Consumer, *Communications of the ACM*, 49 (8), 61-65.
15. Turle, Marcus (2007), Know the Legalities of Biometrics, *Computer Weekly*, (February 20), 26-28.
16. Tynan, Dan (2007), Watch Out for Online Ads That Watch You, *PC World*, 25 (3), 26.