

Behavioral Targeting

April 30, 2009

Donna K. Lewis
donna.lewis@nelsonmullins.com
404.322.6346

**Nelson
Mullins**

Advertising 101

- Size of audience and relevance are key to ROI
- Geographic, demographic and psychographics (attitudes, lifestyles, opinions)
- CPM increases with targeting abilities
- Networks/sites maximize opportunities and revenue
- Advertisers see improved ROI
- Advertising supports (i.e., pays for) content (advertising v. subscription models)

Direct Marketing Across Media

- The direct marketing process involves: the use of data to identify and address like categories, an analysis of that data to develop relevant and effective offers and communications using a variety of addressable media with the ability to track and measure communications and transactions, and the ability to test new methods to improve processes throughout the organization
- Contrast with mass advertising which tends to be inefficient and ineffective in driving sales as opposed to brand building
- National and local sales opportunities exist across media platforms, but buying process is inefficient (patchwork)

Direct Marketing Across Media (Con't)

- National and local broadcast, cable, direct mail, telephone solicitation, print, Internet, wireless (e.g., GPS technology)
- The Internet and availability of ever-increasing amounts of digital data, combined with the development of new technologies to manage and track that data allow the data to be converted into valuable information
- Online behavioral advertising reflects next-generation direct marketing efforts, moving beyond contextual ads (placement based on the content of the Web page, not who is viewing it)

Direct Marketing Spend and ROI

- It works!
- \$173.2 billion spent on DM in the US in 2007
- These DM expenditures generated \$2.025 trillion in incremental sales, accounting for 10.2% of total US GDP
- Each DM dollar yields an average ROI of \$11.69 versus \$5.24 for non-direct marketing
- A fully integrated DM process may increase an organization's overall efficiency from R&D through sales and service

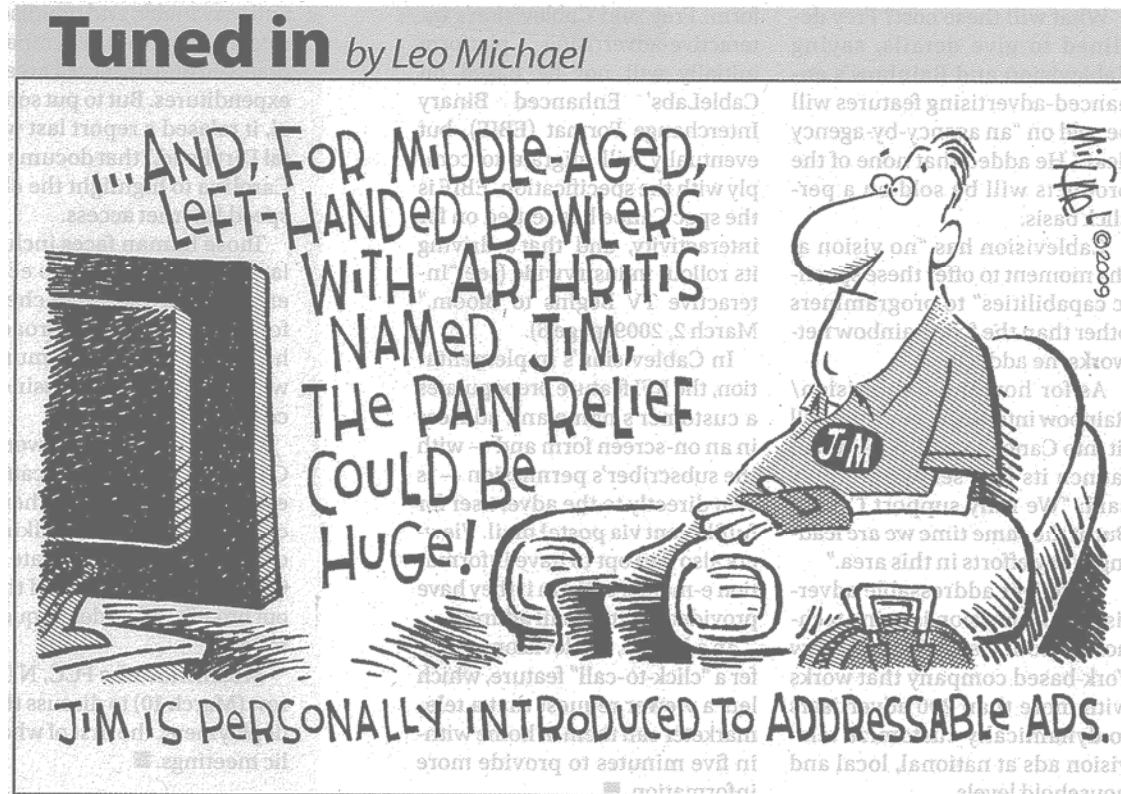
What is Behavioral Targeting?

- Any process whereby data about what you do on the Internet (e.g., search, commerce, postings) is collected to create a profile of your interests
- The profile is stored and used to serve you online ads believed to be more relevant to you
- Relevance is believed to maximize click through rate and sales conversion
- The process has been perceived as threat to privacy and consumer protection
- NAI – "OBA means any process used whereby data is collected across multiple web domains owned or operated by different entities to categorize likely consumer interest segments for use in advertising online"

How It Works

- Data mining involves extracting hidden patterns from data in order to transform that data into valuable information via the use of computer power to apply knowledge discovery methodologies; it is commonly used in profiling practices such as surveillance, marketing, fraud detection and scientific discovery
- Data mining applies knowledge discovery and prediction through a process of classification, clustering, regression and association rule learning
- The value of the information derived through data mining depends on the collection of indicative and representative data
- Data mining has been used with retail scanner data, census data and passenger trip records
- Cookies for behavioral advertising usually contain text that uniquely identifies your browser so that advertisers or ad networks can recognize the same Internet user across different Web sites or multiple areas on the same site

What the Consumer Sees



Applicability of Current Laws

- Common law privacy and trespass
- CAN-SPAM
- Electronic Communications Privacy Act of 1986
 - Intentional interception of contents of electronic communications using a device (e.g., server?)
 - Intentional disclosure of intercepted material with knowledge of acquisition wrongdoing
 - Certain exceptions for necessary incident and ordinary course and consent
- Computer Fraud and Abuse Act
 - Intentional access exceeding authorization to a protected computer in furtherance of a fraud and damages of \$5k; or
 - Intentional transmission of code that accesses a protected computer and causes damages

Applicability of Current Laws (Con't)

- **FTC Act**
 - Section 5 - Unfair and deceptive trade practices
 - Application to spam, spyware, search and pop-up advertising, information security and behavioral advertising
- **Lanham Act**
 - Misrepresentation or omission of material fact that affects purchasing decision and causes damage
- **Video Privacy Protection Act of 1988**
 - Wrongful disclosure of video tape rental or sale records
 - Not preemptive of broader state video privacy law

Applicability of Current Laws (Con't)

- Cable TV Privacy Act of 1984
 - Personally identifiable information (excludes data that is anonymous)
 - Limits collection and disclosure by cable operators (need consent for collection of PII)
- State law equivalents for consumer protection and privacy

The Push Over the Edge

- Traditional focus of Web site policies and practices has been around collection and use of personally identifiable information; sufficient for this level of "intrusion"?
- Publisher's privacy policies often reserved broad rights of use with respect to aggregated, anonymous data
- Profiling has arguably improved through the availability of more information from more sources and advances in processing technology; there is some concern that these advanced data mining capabilities may uncover patterns that compromise confidentiality and privacy
- Growth of social networking sites pose unique challenges
- Risk to traditional protections afforded in connection with sites targeted to children under 13

The Push Over the Edge (Con't)

- More importantly, the actual or perceived increase in use of the information for commercial gain by third parties has led to heightened actual or perceived threats to privacy
- As a result, there is renewed interest in expanding the definition of PII to include IP addresses
- There is also some concern that once the anonymous data from multiple sites and communication sources (e.g., postings) is aggregated, it is possible to re-identify specific individuals
- Use of deep packet inspection (DPI) technology for OBA
 - DPI looks at content; serves legitimate security/network management needs
 - Comcast/Charter experimented with use
- Different privacy expectations for browsing and web sites/portals

Options

- Effective self-regulation by the industry
 - TRUSTe (Internet privacy; EFF)
 - Direct Marketing Association (DMA)
 - Network Advertising Initiative (NAI; third party network advertisers)
 - NCTA
- Regulation
 - Push by The Center for Democracy and Technology (501(c)(3) public policy organization with focus on practical solutions to enhance free expression, privacy and open access in digital global communications)
 - EPIC support for privacy legislation; specifically around DPI usage for OBA
 - US lawmakers discussed proposed privacy legislation last week around DSI

US Activity

- General changes in regulatory environment with a trend towards increased interest in privacy/security matters
- Publication of 2008 NAI Principles
 - Updated for the first time since 2000
 - Implements a more inclusive approach
 - Expands coverage scope beyond behavioral advertising to include multi-site advertising (i.e., ad delivery and reporting – collecting data about a browser for purposes of delivering ads or providing advertising-related services - across multiple web domains owned or operated by different entities)
 - Expanded definition of "sensitive" information to include precise geographic location information (e.g., via GPS-enabled devices) and a broader definition of health information, as well as SSN, government issued identifiers, insurance plan numbers, and financial account numbers

US Activity (Con't)

- Publication of 2008 NAI Principles (con't)
 - Stipulates required content of member notice to disclose activities, data types collected, data use/transfer, types of PII and non-PII that will be merged and how merged data will be used/transferred
 - Approximate period of retention of data suggested
 - Opt-in required for: use of PII merged with previously collected non-PII (retrospective merger) and when using sensitive consumer information
 - Use of non-PII or PII to create OBA segment specifically targeted to children under 13 is prohibited without verifiable parental consent
 - Must provide reasonable security for subject data
 - Implementation guidelines to follow
 - Enforcement – FTC Section 5, consumer complaints, pre-certification and annual compliance review, sanctions

US Activity (Con't)

- CDT Response to 2008 NAI Principles (December 16, 2008)
 - Some progress, but inadequate to address privacy and consumer protection issues
 - Criticize retention of opt-out choice mechanism via cookies; advocate "Do Not Track" list or adoption of a more informed consent standard
 - Inadequate notice requirement of "clear and concise" that is below FTC standards which require a clear, concise, consumer-friendly, and prominent notice

US Activity (Con't)

- CDI Response to 2008 NAI Principles (con't)
 - No requirement for compliance check by third party
 - ISP behavioral advertising unaddressed (collection of all or considerably all of the user's traffic data via ISP DPI process)
 - Multi-site advertising without a choice requirement
 - Data retention not tied to the purpose of collection (FTC takes the same position) but rather as necessary to fulfill a legitimate business need or as required by law
 - Lack of a long-term plan for user controls (ability to review and edit profiles); practical problem; suggestion of a dashboard to increase transparency and controls?

US Activity (Con't)

- FTC Proposed Self-Regulatory Guidelines (2007 with 1-plus year of comments)
- FTC Report (February 12, 2009)
 - Outlines self-regulatory guidelines/principles (final) for online advertising industry
 - Transparency and opt-out choice
 - Provides last chance for self-regulation
 - Applicability of privacy protections to any data that reasonably can be associated with a particular consumer or computer or other device
 - For transparency and consumer control principle (1), the FTC encourages creative and effective disclosure mechanisms separate from web site privacy policies
 - For its material change principle (2), the focus is on retroactive changes
 - Security principle (3) and sensitive information principle (4)

US Activity (Con't)

- TRUSTe Behavioral Targeting Checklist
 - Practices that impact consumer trust
 - Recommendations on "best practices"
- Extension beyond Internet to other digital media
 - Addressable advertising via digital cable
 - Canoe Ventures (cable consortium) allows marketers to buy national ads and send different messages to different demographic groups at the same time (and simultaneously build brand)
 - Aggregate geographic, demographic and psychographic characteristics
- FCC seeking comment on best practices to safeguard consumer privacy in connection with OBA and DPI

General Framework Emerging

- Transparency/notice
- Choice/consumer control
- Privacy protection/reasonable security
- Customer value (relevant advertising = content; provision of support for other products/services of value)
- Retention policies
- Variance across categories: Non-PII, merged with PII (prospective and retrospective), sensitivity, children

Remaining Questions

- What is PII?
- Genuine consumer concern over practice or acceptance of concept (i.e., necessary and here to stay)
- Real or perceived risk to privacy
- Opportunity to do it right – build consumer trust and develop better information and improved ROI on an integrated basis
- Applicability of existing laws
- Sufficiency of self-regulation
- Need for new laws; potential conflicts with existing laws
- Opt-in sufficient?
- Always evolving with technology

EU Activity

- Significant concern
- Privacy paradox – 80% concerned about Internet privacy but doing nothing for protection (TRUSTe data – 68%)
- Google's practices under scrutiny
- Commission actively seeking external advice on Internet privacy
- Call for voluntary code of conduct for online advertising industry; proposal developed by Internet Advertising Bureau (UK-based trade association for media owners and agencies in the UK Internet industry) and 9 Internet companies (including Google, AOL and Microsoft) though it has been criticized as being insufficient
- Significant concern about ISP's use of DPI technology
- EC launched infringement proceeding against member state (UK) for alleged failure to keep online details confidential, following complaints about use of OBA by ISPs

General Framework Emerging

- Unclear
- Talks planned with FTC, Microsoft, Google
- Likely to be more stringent than US framework
- Result – Dual compliance challenges

Acquiring/Maintaining Lists for OBA

- Need clear agreement in place for use of third party list
- List provider should warrant:
 - Information was obtained legally
 - Individuals consented to third party contact
 - No individual revoked consent
- Covenant to notify in the event of future revocation

Acquiring/Maintaining Lists for OBA (Con't)

- Implement reasonable security measures to protect lists
 - Prevent unauthorized access, use and disclosure
 - Include in "incident response" policy
 - Periodic audit/check
- Compliance Requirements
 - Establish system to update revocations
 - Manage retention period
 - System beyond opt-out cookie maintenance required?

Resources

- National Advertising Self Regulatory Code (NAI)
- Center for Democracy and Technology Threshold Analysis for Advertising Practices
- FTC Proposal
- TRUSTe Behavioral Targeting Checklist