EMERGING LEGAL ISSUES ARISING FROM TARGETED BEHAVIORAL ADVERTISING

© Etahn M. Cohen

Sugar & Felsenthal LLP

Chicago Bar Assn., June 16, 2009

What is Behavioral Advertising?

- Also called Behavioral Marketing or Behavioral Targeting
- FTC defines behavioral advertising as “the practicing of tracking a individual’s online activities in order to deliver advertising tailored to the individual’s interests”
- Tracking may not just be one session but many

Rationale for Tracking

- The rationale is that the more data the advertiser has on the person browsing, the more they can focus the ad on the person's interests
- See "To Aim Ads, Web is Keeping a Closer Watch on You", *New York Times*, March 10, 2008
- More effective than other types of online ads
- Advertisers pay more for ads arising out of targeted marketing

How does it work?

- The primary method is cookie-based and/or use of web bugs
- Information collected includes web pages a person visits, content viewed and searches that a person conducts
- Sometimes additional data if registered at a site
- Networks of sites contributing information and hosting ads

Web Bugs

- A one-pixel image on a web page
- Refers to another server
- In a non self-contained web page, the computer viewing the web page goes out to other server to obtain this image
- The other server records the IP address of the computer making the request

Nature of the Tracking

- Based usually only on the IP address of the individual's computer and not name or other personally identifiable data
- However, since tracking programs record IP address of computer being served, data can be collected even if cookies turned off
- Cookies may be less relied upon because anti-spyware deletes many tracking cookies

Example of Tracking

- Went to BlueKai Website
- Actually an intent data exchange
- Registry showed that my computer was associated with both international and domestic travel
- Allowed me to opt-out
- McAfee Security software found no tracking cookies
- www.bluekai.com/consumers.html

Example: AudienceScience

- 345 million unique users
- Recording billions of behavioral events daily
- Users broken up into various market segments:
  - **AUTO:** Auto Enthusiasts; Hybrid Car Shoppers European Import Buyers
  - **ENTERTAINMENT:** Sports Lovers, DVD Buyers, TV Enthusiasts
  - **TRAVEL:** Business Travelers, Vacation Travelers International Travelers

Possible Criteria for AudienceScience Advertisers

- Behavioral
- Creative
- Re-Targeting
- Geographic (Salon.com ad to Wilmette residents by Pulse360)
- Day-Part
- Demographic
- Connection Speed
- Channel
- SIC Code

Benefits to Consumer

- Supports free online content
  - Important point given that Facebook, Twitter, Digg, Youtube and many other highly popular sites do not presently make money
- Personalized advertising that many consumers may value
- Potential reduction in unwanted ads

Nature of Concerns with Behavioral Advertising

- Invisibility of tracking to consumers
- Lack of adequate disclosure regarding tracking
- Lack of consumer control of tracking
- The potential to develop and store profiles about consumers
- The risk that data collected – including sensitive health or financial data – could fall into the wrong hands

Broad Concerns about Online Privacy

- Concerns with online privacy have been expressed in public opinion polls, complaints to regulatory bodies, bills introduced in Congress and state legislatures, FTC hearings and Congressional hearings
- The FTC has been the most consistent observer of this area

TRUSTe Survey of Online Privacy

- 90% of respondents called online privacy a “really” or “somewhat” important issue
- Only 28% stated that they were comfortable with behavioral targeting – defined as when advertisers used browsing history or search history to decide what ads to show them
- 51% said they were not comfortable with behavioral advertising (decline from 57% in prior year)

Public Internet Privacy Concerns

- Data from knowprivacy.org
- Collaborative project of graduate students from UC Berkeley School of Information
- A comparison of users' expectations of privacy online and the data collection practices of website operators.

User Expectations and Knowledge from Study

- Users are concerned about data collection online and want greater control over their personal information
- Users lack awareness of some data collection practices
- Users don't know who to complain to

Website Practices from Study

- Websites collect and analyze data about users, but only offer partial access and control to the users
- Website policies are unclear about several important issues, such as retention and data enhancement

(continued)

- Websites claim they do not share user data with third parties, but they do share with affiliates that users may have no relationship with
- Web bug trackers are ubiquitous. Analytics and ad serving companies can track user behavior across large portions of the web

Sites with most web bugs
(March 2009)

Domain	Web Bugs
blogspot.com	100
typepad.com	75
google.com	44
blogger.com	31
msn.com	29
aol.com	28
yahoo.com	27
huffingtonpost.com	27
photobucket.com	25
tripod.com	25

Web Bugs on Sites in Study

Tracker Coverage Across Top 100 Sites
(March 2009)

Tracker	Percent
Google Analytics	81%
Doubleclick	70%
Microsoft Atlas	60%
Omniture	57%
Quantcast	57%
PointRoll	54%
Google Adsense	52%
Dynamic Logic	48%
Insight Express	41%
ValueClick Media	41%

Congressional Concern with Online Privacy

- On April 23, 2009 the House Energy and Commerce Subcommittee on Communications, Technology and the Internet held a hearing on online technologies including deep packet inspection technology – examination the data portion of internet traffic
- On July 9, 2008 the Senate Committee on Commerce, Science and Transportation held a hearing entitled “Privacy Implications of Online Advertising”

Possible Legislation

- Rep. Boucher in a speech to Computer and Computer Industry Association indicated that he was planning to reintroduce his bill on offline as well as online data collection
- Previously introduced a similar bill in the 109th Congress with Rep. Stearns

Proposed NY Legislation

- 2008 bill in the NY Assembly (A. 9275) and Senate (S.6441)
- Called Third Party Internet Advertising Consumers' Bill of Rights Act of 2008
- Based on Network Advertising Initiative (NAI) self-regulatory principles
- Notice and opt-out main provisions

Competing Self-regulatory Guidelines

- NAI Guidelines discussed above
- Interactive Advertising Bureau – an organization of comprising many leading Internet companies – has proposed self-regulatory guidelines similar to the FTC guidelines

Interest Group Guidelines

- Center for Democracy and Technology has issued its Privacy Principles for Development of User Controls for Behavioral Targeting

FTC Town Halls on Behavioral Advertising

- Since 1995 the FTC has been active in understanding the online marketplace and the privacy issues it raises
- In November, 2007 the FTC held a Town Hall on Behavioral Advertising
- Meeting included behavioral advertising users as well as privacy advocates

Draft Behavioral Advertising Principles

- In December, 2007 FTC issued draft principles designed to serve as the basis for industry self-regulation to address privacy concerns
- FTC sought comments on the guidelines

1. Transparency and Consumer Control

- Every website where data is collected for behavioral advertising should provide a clear, concise, consumer-friendly, and prominent statement that (1) data about consumers' activities online is being collected at the site for use in providing advertising about products and services tailored to individual consumers' interests, and (2) consumers can choose whether or not to have their information collected for such purpose. The website should also provide consumers with a clear, easy-to-use, and accessible method for exercising this option.

2. Reasonable security, and limited data retention, for consumer data

- Any company that collects and/or stores consumer data for behavioral advertising should provide reasonable security for that data. Consistent with the data security laws and the FTC's data security enforcement actions, such protections should be based on the sensitivity of the data, the nature of a company's business operations, the types of risks a company faces, and the reasonable protections available to a company.

2. continued

- Companies should retain data only as long as is necessary to fulfill a legitimate business or law enforcement need.

3. Affirmative express consent for material changes to existing privacy promises

- A company must keep any promises that it makes with respect to how it will handle or protect consumer data, even if it decides to change its policies at a later date. Therefore, before a company can use data in a manner materially different from promises the company made when it collected the data, it should obtain affirmative express consent from affected consumers. This principle would apply in a corporate merger situation to the extent that the merger creates material changes in the way the companies collect, use, and share data.

4. Affirmative express consent to (or prohibition against) using sensitive data for behavioral advertising

- Stakeholders express concern about the use of sensitive data (for example, information about health conditions, sexual orientation, or children's activities online) to target advertising, particularly when the data can be traced back to a particular individual. They state that consumers may not welcome such advertising even if the information is not personally identifiable; they may view it as invasive or, in a household where multiple users access one computer, it may reveal confidential information about an individual to other members.

FTC Staff Report

- On February 12, 2009 the FTC released the Staff Report on Self-Regulatory Principles for Online Behavioral Advertising
- Refined original draft principles

Status of FTC Principles and Report

- FTC generally in favor of industry self-regulation
- Like the original principles, the report imposes no legal obligations and does not have the status of rule or regulation
- Report and principles give indication of business practices that would likely to attract staff attention
- Two commissioners stated that more formal regulation or legislation would be in order if industry practices do not conform more closely to staff recommendations

Applicability to Non-PII

- Do the Principles only apply to personally identifiable information (PII)?
- FTC believes that the non-PII raises privacy concerns and that the distinction between the two is no longer as meaningful
- Combining enough non-PII information will allow linking of non-PII to a person

The AOL Search Data Incident

- In 2006 AOL made public some 20 million search queries conducted by subscribers over 3 month period
- Data posted on the web
- Individuals identified with this information

FTC Position on Non-PII

- FTC desires to include within the principles “any data collected for online behavioral advertising that reasonably could be associated with a particular consumer or a particular computer or device”
- What is “reasonably could be associated” data?
- Consistent with the NAI position

Principles not Apply to "First Party" Online Behavioral Advertising

- "First Party" behavioral advertising practices were deemed consistent with consumer expectations
- Principles only apply to tracking of consumers' activities across different websites
- Or if website shares data on consumers

Principles Not Applicable to Contextual Advertising

- FTC determined that ads based solely on the page that a consumer is visiting or on the search that the consumer has just carried out does not raise the same issues other behavioral advertising
- Less risk because these types of ads do not require the collection of detailed information about consumer behavior over time
- Benefits of excluding this practice from Principles outweigh risks where data is not stored

Consumer Choice on Collection of Non-PII

- FTC position is that companies should provide consumers choice for collection of data online behavioral advertising if “the data reasonably could be associated with a particular consumer or with a particular computer or device”
- Significant controversy with respect to this position

Providing Effective Notice and Choice

- Substantial differing opinions on notice and choice regarding data collection
- Privacy policies criticized as an ineffective means of disclosure
- FTC encouraged companies to design innovative ways to disclose data collection outside of privacy policies

Behavioral Marketing Outside of the Traditional Website Context

- Issue of behavioral marketing in the mobile phone area
- Need to create disclosure of data collection on a mobile phone that would be appropriate to a small screen
- The lack of staff guidance in this area means that the industry may devise new means of disclosure that the staff might find inadequate

Reasonable Security and Limited Data Retention for Consumer Data

- FTC in favor of limited retention of data
- FTC thinks security precautions should be scaled to the type of data

Affirmative Express Consent for Material Retroactive Changes to Privacy Promises

- FTC maintains that the failure to do this constitutes an unfair trade practice
- FTC does not think there is a need for such consent if the new policy only applies to new data collected
- Unclear what this means with respect to non-PII
- If non-PII, how do you get consent?

Consistent with In re Gateway Learning Corp. FTC File No. 042-3047

- FTC action that stands for the a company should obtain “affirmative express consent” from its customers where it makes a change in the use of “previously collected” data

Express Consent to (or Prohibition Against) Use of Sensitive Information

- Lack of agreement on what constitutes "sensitive information"
- Existing regulatory schemes do not address most types of online behavioral advertising or the privacy concerns that such advertising raises

Examples of Behavioral Marketing Firms

- AudienceScience (fka RevenueScience)
- Valueclick
- Tacoda
- Google Doubleclick
- See other members of the NAI

Examples of Behavioral Marketing with Legal Issues

- Facebook Beacon
- Valentine v. NebuAd, Inc.
- Simon v. AdZilla, Inc.
- Phorm
- In re Sears Holding Management Co. (FTC proceeding)

Facebook Beacon

- Beacon was an advertising system using Facebook cookies and a 1x1 gif web bug
- The system would send data from external websites to Facebook for the purpose of allowing targeted advertising and to allow users to share their browsing and shopping with their friends

Reaction to Facebook Beacon

- Facebook users quickly protested
- In reaction, Beacon was changed so that any activities published would require explicit permission by the user
- Beacon changed to an opt-in system

Class Action Lawsuit Against Facebook

- Class action lawsuit against Facebook, Blockbuster Inc., Fandango and others
- Claimed violation of Video Privacy Protection Act, Electronic Communications Privacy Act, Computer Fraud and Abuse Act, California Consumer Legal Remedies Act and California Computer Crime Law

Class Action Lawsuit vs. NebuAd, Inc.

- Valentine v. NebuAd, Inc. et al., CV 08 5113 District Ct. for the Northern District of CA
- NebuAd worked with ISPs so that ISPs could intercept and analyze ISPs' subscriber's online transmissions (deep packet inspection technology)
- Deep packet inspection technology analyzes the contents of websites being transmitted through the ISP for targeted advertising

Other Aspects of NebuAd System

- Ties a consumer's individual record at the ISP with a alphanumeric code to uniquely and persistently identify individuals
- Monitors pages visited, search terms entered and words that appear on page
- Ensures that a Web browser is always preloaded with cookies providing unique identifying codes representing the ISP subscriber

Issues with the NebuAd System

- No user consent or knowledge
- Adds cookies by altering the response from the server that the browser is accessing and adding its own cookies
- NebuAd system used forged IP packets that are added onto the response and made it appear to come form the original server
- Able to circumvent the issue of cookie deletion

Lawsuit Allegations

- ISP saw this as a way to obtain some of the Web publishers' revenues
- Lawsuit alleged violations of Electronics Communications Privacy Act, Computer Fraud and Abuse Act, California Invasion of Privacy Act and California Computer Crime Law
- Started to lose ISP when Congress held hearings
- NebuAd, Inc. has gone out of business

Simon v. AdZilla, Inc.

- Simon v. AdZilla, Inc. et al, filed February 27, 2009, Northern District of CA, Case C09-00879
- Case based on use of deep packet inspection

Nature of the Complaint

- Lawsuit alleged violations of Electronics Communications Privacy Act, Computer Fraud and Abuse Act, California Invasion of Privacy Act and California Computer Crime Law
- Wrong was the interception, copying, transmission and alteration of personal, private data of internet subscribers without their consent

Phorm

- Proposing the use of another deep packet analysis technology called Webwise for target advertising similar to NebuAd technology
- Been in talks with ISPs in the United Kingdom
- UK Information Commissioner has ruled that Phorm is only legal as an opt-in system
- EU Communications Commissioner has been concerned that Phorm violates EU laws

In re Sears Holdings Management

- Sears Holding Management Co. (“SHMC”) entered into an agreement containing a consent decree with FTC to settle charges
- FTC alleged that failed to disclose adequately the scope of consumers’ personal information it collected via a downloadable software application
- http://www.ftc.gov/os/caselist/0823099/index.shtm

Specific Issues

- FTC charges that the software would also monitor consumers' online secure sessions – including sessions on third parties' Web sites – and collect information transmitted in those sessions, such as the contents of shopping carts, online bank statements, drug prescription records, video rental records, library borrowing histories, and the sender, recipient, subject, and size for web-based e-mails.

FTC Complaint

- Sears did not disclose that the software would track a participant in the programs on-line browsing
- Issue was that amount of material that was being tracked was not disclosed except in the middle of a voluminous license agreement

Text of FTC Remedy

- IT IS ORDERED that respondent … in connection with the … dissemination of any Tracking Application, shall …:
- A. Clearly and prominently, … on a separate screen from, any final "end user license agreement," "privacy policy," "terms of use" page, or similar document, disclose: (1) all the types of data that the Tracking Application will monitor …; (2) how the data may be used; and (3) whether the data may be used by a third party; and

Remainder of FTC Remedy

- Obtain express consent from the consumer to the download or installation of the Tracking Application and the collection of data by having the consumer indicate assent to those processes by clicking on a button or link that is not pre-selected as the default option and that is clearly labeled or otherwise clearly represented to convey that it will initiate those processes, or by taking a substantially similar action.

Summary

- Few legal prescriptions governing behavioral advertising
- Unlikely that deep packet inspection technology will be allowed
  - Lawsuits still pending
  - Exception is Gmail
- Only clear thing is that more discussion in this area to come

Advise to Clients

- Update your privacy policy to disclose behavioral marketing affiliation or relationship with a behavioral marketing network
- Consider more effective means of notification of behavioral marketing than privacy policy disclosure
- Allow website users to opt-out of having their information collected for behavioral marketing