SO PRIVATE, SO PUBLIC: INDIVIDUALS, THE INTERNET & THE PARADOX OF BEHAVIORAL MARKETING

Remarks of Commissioner Jon Leibowitz
at the
FTC Town Hall Meeting on
"Ehavioral Advertising: Tracking, Targeting & Technology"
November 1, 2007

Good Morning. I'm Jon Leibowitz, one of the FTC Commissioners.[1]

Let me start by thanking the first panel for setting out some of the issues that this workshop will grapple with. As you can tell, reasonable people approach behavioral marketing from very disparate perspectives. Let me also thank *all* the participants in this Town Hall meeting – you are an impressive group and your presence is a testament to the "white heat" of these issues. And finally, a big thank you to the Commission staff for its hard work in organizing this event.

We all bring different privacy expectations to the table:

- It doesn't especially bother me that Amazon keeps track of the books I've ordered and recommends new ones – that's targeted advertising. And it doesn't bother me that search engines deliver sponsored links based on my queries – that's targeted advertising, too.

- Somewhat more disturbing is the new Internet telephone service that uses voice recognition technology to monitor phone conversations and send targeted ads to the subscriber's computer screen during the call.[2] But this service is ***opt in,*** the product is new, and there are plenty of competitors offering telephone service with different privacy practices.

---

[1] The views expressed here are my own and do not necessarily represent the views of the Federal Trade Commission or of any other Commissioner.

[2] Louise Story, *Company Will Monitor Phone Calls to Tailor Ads*, N.Y. Times, Sept. 24, 2007 (Business Section). Pudding Media, a Silicon Valley start-up, asks users for their sex, age range, native language and ZIP code when they sign up for the service so it can better target the ads. Pudding Media is also working on a way to email the ad to the person on the other end of the line or display it on that person's cellphone screen. *Id.*

- I *am* concerned, though, when my personal information is sold to or shared with third parties – or when my online conduct is monitored across several websites or across different web-based services – especially when there is no effective notice or consent to these practices.

- And it should *really trouble all of us* that seemingly anonymous searching and surfing can be traced back to specific individuals – and that not all information that companies have collected about us is secure from data breaches or release.[3]

Don't take my word for it; just ask AOL customers.

Last year AOL released a cache of supposedly anonymized search records, but some people were identified based on their queries. The results were somewhat embarrassing, and it could have been much worse.

In my view, all this is a real paradox: you can go online from the privacy of your home and enter searches or surf websites that involve your sensitive medical conditions or reveal your deepest secret desires – or even your most trivial curiosities. You can create a personal profile on a social networking site and reserve access only for your close friends and family. It all *seems* so private – but because online marketers are tracking our Internet searching, surfing and socializing, it may be more public than we would like to think.

If you have teenagers, you probably know the texting acronym "pos" – parent over shoulder. Well, when you are surfing the Internet, you never know who is peering over your shoulder. Or how many are watching.

To be fair, most of our web searching and browsing and social networking is free – thanks in large part to advertising – and most consumers seem to like it this way. As the Internet has evolved, the ad targeting has become more sophisticated, arguably bringing greater benefits and a richer Internet experience to consumers.

But the question is: at what cost? Are we paying too high a price in privacy?

In his seminal 1983 book, *The Rise of the Computer State*, David Burnham worried that detailed data bases and the expanding network of computerized record systems were enabling large organizations to track the daily lives of individual citizens.

---

[3] Over the past few years, the FTC has initiated more than a dozen enforcement actions against online and brick-and-mortar companies for failure to provide adequate security for sensitive consumer data.

And that was *then* – the Jurassic Age of big mainframes – when personal computers were just entering the market, the Internet was still an academic/military experiment, and AT&T was *the* commercial telecommunications behemoth.

Of course, some things never change.

And some things never stop changing. Today, the Internet, computerized data collection, and targeted advertising are creeping into nearly every aspect of our social and commercial transactions. Seventy-one percent of U.S. adults use the Internet.[4] Nearly half of all Americans have broadband at home.[5] Internet advertising revenues for the first half of 2007 were nearly $10 billion – a 26 percent increase over the first half of 2006.[6] Make no mistake: the business of online behavioral marketing is big business.

In *An Ideal Husband*, Oscar Wilde wrote, "Private information is practically the source of every large modern fortune."

That's especially true today with online behavioral marketing. Just last week, Microsoft announced a $240 million agreement that gives it exclusive rights to sell worldwide ads targeting Facebook's 50 million members. Google already invested $900 million in MySpace, which announced that it can tailor ads based on what users write on their profile pages.[7] Meanwhile, Google is trying to buy online ad server Double Click, Microsoft acquired aQuantive, and Yahoo purchased Right Media. With all these big-money deals comes big-time pressure to push more – and more effective – ads on the Internet.

Collectively, all this tracking of our online conduct – our searching, web browsing, social networking, emailing, and telephone chatting – all this *massive collection of our private information,* purportedly to serve precision-guided ads, can be disconcerting.

---

[4] Pew Internet & American Life Project, *Demographics of Internet Users* (last updated June 15, 2007), available at http://www.pewinternet.org/trends/User_Demo_6.15.07.htm.

[5] John B. Horrigan & Aaron Smith, Pew Internet & American Life Project, *Home Broadband Adoption 2007* (June 2007) (Data Memo), available at http://www.pewinternet.org/pdfs/PIP_Broadband%202007.pdf

[6] Interactive Advertising Bureau, Inc., press release, *Internet Advertising Revenues Continue to Soar, Reach Nearly $10 Billion in First Half of '07; Historic Second Quarter Revenues Exceed $5 Billion for First Time* (Oct. 4, 2007)**.**

[7] Brad Stone, *MySpace Mining Members' Data to Tailor Ads Expressly for Them,* N.Y. Times, Sept. 18, 2007, at C1.

Perhaps it is because we don't quite understand what websites and online advertisers are doing or how they are doing it. Perhaps it is because we feel like we don't really have any meaningful choice or control in the matter – other than to stay offline. Perhaps it is because we don't really know what information websites and others have collected about us. Perhaps it is because we have no assurance that they will protect the security and confidentiality of our sensitive personal or financial information.

When the Commission first confronted these issues nearly a decade ago, there was general acceptance of four core "fair information practice principles": notice, choice, access, and security.[8] Industry efforts to implement these principles resulted in many websites developing and posting so-called privacy policies.

Initially, privacy policies seemed like a good idea. But in practice, they often leave a lot to be desired. In many cases, consumers don't notice, read, or understand the privacy policies. They are often posted inconspicuously via a link at the very bottom of the site's homepage – and filled with fine-print legalese and technotalk.

A recent study submitted as a comment for this Town Hall examined privacy policies of Fortune 500 companies and found that they were essentially incomprehensible for the majority of Internet users.[9] Only one percent of the privacy policies were understandable for those with a high school education or less (like most teens and many consumers). Thirty percent of the privacy policies required a post-graduate education to be fully understood.[10]

The study also found that fewer than 27 percent of the privacy policies allowed consumers to opt-out of collection of data. ***None of the privacy policies surveyed allowed consumers to opt in. Not one.***[11] The vast majority of the privacy policies simply

---

[8] FTC, *Privacy Online: A Report to Congress* (1998). The Commission also identified **enforcement** – the use of a reliable mechanism to identify and impose sanctions for noncompliance with these fair information practices – as a critical ingredient in any governmental or self-regulatory program to ensure privacy online. *Id.*

[9] Felicia Williams, *Internet Privacy Policies: A Composite Index for Measuring Compliance to the Fair Information Principles* at 17 & Table 2 (Sept. 2006) (submitted as a public comment to the FTC on Oct. 10, 2007).

[10] *Id.*

[11] *Id.* at 26. Fifteen percent of the privacy policies stated the firm would obtain permission before sharing or selling collected data.

state that consumers signify their acceptance to the collection of data by using the website.[12]

Your only choice: take it or leave it.

Even the title "privacy policy" is arguably a misnomer in some cases because many consumers believe that the term "privacy policy" means that the website will protect their privacy and will not share their information.[13]

All the online tracking and targeting is especially worrisome when it involves our children. A whopping 93 percent of American teens age 12 to 17 use the Internet – and 55 percent of these online teens use social networking sites.[14] Internet use by children even younger is growing as well. When Congress passed the Children's Online Privacy Protection Act, it clearly recognized that young children deserve special protections in cyberspace. To that end, COPPA imposes certain requirements before websites may collect personal information from children under the age of 13.

But today, is that really enough?

Based on the focus group I convened over the weekend – that is, my 12-year-old daughter and four of her friends – the online ads that target children aren't always appropriate for their age. They see ads with titles like, "How Long Is Your Next Kiss," and "Touch Me Harder." The FTC's most recent Report on marketing violent entertainment products to children seems to confirm some disturbing practices in this area. For example, sites like MySpace ran banner ads for R-rated movies, even though the site reaches a large number of children under 17.[15]

---

[12] *Id.* at 27.

[13] In fact, some privacy experts have argued that the "privacy policy" label is deceptive unless the website obtains affirmative consent from consumers before sharing their personal information. Joseph Turow, Chris Jay Hoofnagle, Deirdre K. Mulligan, Nathaniel Good & Jens Grossklags, *The FTC and Consumer Privacy In the Coming Decade,* at 18-19 (Nov. 8, 2006), available at http://www.ftc.gov/bcp/workshops/techade/pdfs/Turow-and-Hoofnagle1.pdf.

[14] Amanda Lenhart, Pew Internet & American Life Project, *A Timeline of Teens and Technology*, presented at APA Policy and Advocacy in the Schools Meeting at 4, 21 (Aug. 16, 2007), available at http://www.pewinternet.org/ppt/APA%20School%20Psychologists_Teens%20and%20Tech_081607revsf1nn.ppt.

[15] FTC, *Marketing Violent Entertainment to Children: A Fifth Follow-up Review of Industry Practices in the Motion Picture, Music Recording & Electronic Game Industries* at 6,

We enacted COPPA to place a parental buffer between advertisers and our children – but the rise of sophisticated behavioral marketing techniques is eroding this parental control.

So what should the Commission do?

Well, sometimes the answer to problems in cyberspace is clear, like in the case of unfair and deceptive nuisance adware. Put the malefactors under order. Disgorge their profits. Pass a law giving the FTC the authority to impose fines.

For behavioral marketing, the solution is not so certain. Behavioral marketing is complicated. In some cases the privacy tradeoff may make sense. But one thing is clear: the current "don't ask/don't tell" mentality in online tracking and profiling needs to end.

And while I don't presume to have all of the answers, I do have a few thoughts: let's start with providing better information and more meaningful choices for consumers.

- Standardized Privacy Policies & Shorter Notices. First, some have called for standardized privacy policies – including former Commissioner Sheila Anthony.[16] And some have called for shorter notices.[17] The take-away from the Commission's recent workshop on "negative option" marketing was that short, conspicuous online notices work better for consumers. All these ideas are worth exploring in the behavioral marketing context.

- Opt In Rather Than Opt Out. Another improvement would be for more firms to allow consumers to "opt in" when it comes to collecting information – especially when it comes to sharing consumer information with third parties and sharing it across various web-based services. Consider changing the widespread opt-out default for ad-serving cookies – ***why not make it opt in?*** At this point, I'm not sure that government should mandate an opt-in model but, in my view, it is a far more preferable result.

- More Competition to Protect Privacy. There is some good news here too. With all the attention on online data collection these past few months, the leading search engines

---

11 (Apr. 2007), available at http://www.ftc.gov/reports/violence/070412MarketingViolentEChildren.pdf.

[16] Sheila F. Anthony, *The Case for Standardization of Privacy Policy Formats*, available at www.ftc.gov/speeches/anthony/standardppf.shtm; *see also* Williams, *supra* note 9, at 56.

[17] *E.g.*, Turow et al., *supra* note 13, at 12-13.

have been tripping over each other to have the strongest privacy protections. For example, Google announced in March that it would anonymize its server logs after 18 to 24 months — so that search histories can no longer be identified with individual users.[18] A few months later, Microsoft announced it would make search queries anonymous after 18 months. Within days, Yahoo announced its plans to make users' search history anonymous within 13 months. Ask.com announced that it will offer a new feature – AskEraser – that will allow users to erase their search histories at will.

Let's hope we see more competition to give consumers more understandable information, more choice, and more control. Indeed, today's Town Hall already inspired a number of creative new approaches, including a "Do Not Track" list. We do need to take a closer look at this, of course, but it's the kind of idea we were hoping our Town Hall would spur.

■ Enforcement When Necessary. It's always great when the competitive marketplace can solve these types of problems, although my sense here is that the market alone may not be able to resolve all the issues inherent in behavioral marketing. So at the Commission, we will listen closely to what online marketers are doing, how they are doing it, and who they are doing it to – and we will think about how to ensure all the wonders of the Internet while respecting consumers' sense of privacy.

We will also continue to monitor industry behavior – and if we see problematic practices, the Commission won't hesitate to take action to protect consumers.

Thank you.

---

[18] The Official Google Blog, *Taking Steps to Further Improve Our Privacy Practices* (Mar. 14, 2007), available at http://googleblog.blogspot.com/2007/03/taking-steps-to-further-improve-our.html.