

**“Where’s the Remote?
Maintaining Consumer Control in the Age of Behavioral Advertising”**

**Remarks of FTC Chairman Jon Leibowitz
As Prepared for Delivery
at the
National Cable & Telecommunications Association
The Cable Show 2010
Los Angeles, California
May 12, 2010**

Thanks to Kyle McSlarrow and the NCTA for inviting me to be here.

It is a pleasure to speak to you today. As leaders in the delivery of entertainment, as the largest providers of high speed Internet, as suppliers of digital telephone service – you have given consumers new, expanded, and innovative ways to relax, enjoy, shop, do business, communicate, share, and learn.

When I was growing up, he who controlled the TV remote, controlled the universe. Come 5 PM, that person had the awesome responsibility of deciding between local news, local news, local news – and Batman. Today, I can – anytime – go to my cable on-demand channel and watch any movie nominated for an Academy Award in the last 20 years. My wife can check out the London Times using the free wi-fi at the corner coffee shop. And my daughters can watch “David After Dentist” on YouTube ... for the 200th time.

Every day, cable companies are investing heavily to deliver precisely the content consumers want, when and how they want it. Consumer choice. Consumer control. These are the principles that underpin the wild popularity of new and newer media. These are the engines that fuel the drive for ever more creative content and ever more inventive ways to deliver it.

Consumer choice and control also lie at the heart of what I am here to talk to you about today: behavioral advertising – a practice with well understood, ancient roots, but some veiled and disturbing implications for privacy when undertaken in ever-expanding cyberspace.

As far back as the 4th Century BC, Aristotle was exhorting those with something to sell to learn about those they hope to sell to.¹ And, in its most basic sense, isn’t that what behavioral

¹ According to Aristotle:

We must also take into account the nature of our particular audience when making a speech of praise; for, as Socrates used to say, it is not difficult to praise the Athenians to an Athenian audience. If the audience esteems a given quality, we must say that our hero has that quality, no matter whether we are addressing Scythians or Spartans or philosophers. Everything, in fact, that is esteemed we are to represent as noble. After all, people regard the two things as much the same.

advertising is? Ads targeted to a receptive audience. They are usually good for consumers, who don't have to waste their time slogging through pitches for products they would never buy; good for advertisers, who efficiently reach their customers; and good for the Internet, where online advertising helps support the free content everyone enjoys and expects.

But things are more complicated in cyberspace, where we scatter crumbs of personal information wherever we go. Here, behavioral advertising can strike at the heart of consumer choice and consumer control – the ability of consumers to choose whether and what private data to share – the ability of consumers to control that data when they do share it.

Imagine you are walking around the mall – and right behind you is a man watching each item you look at or touch. Into his cell phone he keeps up a running commentary: “He’s going for the running shorts ... wow, in lime green ... looks like he might be thinking about losing some weight ... you guys down at the supplement store may want to push the acai berry when he walks by ... oh good, he’s got a platinum Visa ...” If it is you he’s following, you might be annoyed, or a little shaken, or worried what he was going to do with all that information he’s so freely sharing with other merchants. If it is your daughter he’s following, you punch the guy out. You may have no explicit idea what he’s up to or what harm his activity might do, but can anyone seriously assure you that there absolutely, positively can’t be anything to worry about?

Yet isn’t this what happens – or could happen – any time a consumer goes online to get information or make a purchase?

Behavioral advertising raises questions of consumer choice. Consumers often have no idea that advertisers are charting their personal information. If they are told, it is often through a small print disclosure or user license agreement full of legalese.

Behavioral advertising also raises questions of consumer control. Once advertisers capture personal data, consumers have no say in where or how securely it is stored. And they have little or no recourse if – or when – the data is stolen.

We keep hearing about data security breaches in the news, and each breach we hear about is one too many. The Federal Trade Commission has brought almost 30 data security cases to date against companies that did not properly safeguard personal information. One recent case was against T.J. Maxx after allegedly lax security resulted in the release of information on tens of millions of credit and debit cards and in tens of millions of dollars of fraudulent charges.

Data security, to be sure, is a problem bigger than behavioral advertising. But it is also a problem that any serious examination of behavioral advertising must acknowledge.

It has been a challenge for us to come up with the right framework to analyze behavioral advertising. In the FTC’s more traditional consumer protection work, we often look to stop practices that cause consumers tangible harm. But wouldn’t that miss a serious part of the value of privacy to consumers? How can we put a price on the unease of knowing that strangers out in cyberspace might be compiling detailed dossiers about you? Going back to the mall, how would you feel if, when you complained to mall security, they said, “Come back when you can prove,

and quantify, what harm he has actually done”? You might decide to patronize another mall – if one is available. But you surely wouldn’t feel satisfied with that answer.

In simpler times, notice and consent was the standard bulwark for consumer privacy. Marketers gave consumers truthful information so they could decide what they wanted to buy, how much they wanted to pay, and with whom they wanted to do business.

And that works – when consumers understand the information they are receiving and what they are consenting to. But today, few of us can comprehend the amount of personal data we’ve left open for capture on the Internet, and disclosure forms are most often written by lawyers, paid, it seems, by the syllable. The consent half of “notice and consent” rarely reflects a consumer’s conscious informed choice.

This became clear to us during a case we brought last year. The FTC sued Sears after the company paid \$10 to consumers who visited the company’s Sears and Kmart websites and agreed to download software that the company said would confidentially track their online browsing. In fact, the FTC charged that the software collected information on almost all Internet usage, including the contents of consumers’ shopping carts, online bank statements, drug prescription records, video rental records, passwords, library borrowing histories, and even the sender, recipient, subject line, and size of web-based email messages. Only in a lengthy user license agreement, available to consumers at the end of a multi-step registration process, did the company disclose the extent of the information the software tracked.

How many of the consumers who signed up do you think read that? How many do you think knew that the extensive data mining Sears and Kmart apparently were engaged in was possible? How often have you clicked on “agree” to the terms and conditions for entering a website without looking at them? Please raise your hands.

To ask the question is to answer it.

No one looking at the facts of this case can argue that customers made a conscious and informed choice to be subject to such invasive monitoring – which highlights how challenging it is to obtain meaningful consent from consumers, even when they do opt-in to participate.

We know that those of you in the industry are much better positioned to understand the threats to consumer privacy – and to put in place the technical safeguards that I believe we all want.

And we have great hopes for self-regulation. Last year, a coalition including the Direct Marketing Association, the Interactive Advertising Bureau, and the Better Business Bureau proposed behavioral advertising guidelines; these included the recommendation that companies explain their information collection practices for advertising outside the privacy policy using common language and a common icon. So long as self-regulation is making forward progress, the FTC is not interested in regulating in this area.

The FTC does not want to shut down responsible business practices or stifle innovative and efficient uses of the online marketplace – and we don't plan to do so. We want only, as behavioral advertising develops and spreads, to protect those two pillars of the growing, changing, thriving cyber-world: consumer choice and consumer control.

However, there is still work to be done. I have said for a while that Congress will step in if the industry's self policing does not adequately protect consumer choice and consumer control. This is exactly what seems to be happening: last week Representative Boucher from Virginia released a discussion draft of legislation that would regulate online data collection. We expect Congress to discuss this legislation, and the topic of online privacy in general, in the months to come.

So what are we doing at the FTC? Last year, the FTC staff issued a revised set of behavioral advertising self-regulatory principles based on a workshop we held and comments from industry members, privacy advocates, and other stakeholders. The principles are simple and reasonable.

First, each website gathering information for behavioral advertising needs to tell consumers that's what it is doing – and allow them to choose whether they want their data collected for that purpose. And by this, I do not mean another 3-point font, ten-page document written by corporate lawyers and buried deep within the site. My daughters can go to any of a number of retail clothing websites, and, with one click, see a clear description – color, sizes, fit, customer reviews, shipping options – of a pair of pants. One more click and they can choose exactly the pants they want, in their sizes and favorite colors, shipped where they want them.

Put the guy who designed *that* page on the job of presenting a meaningful disclosure and consent form.

Second, companies that collect consumer data should store it securely and keep it only as long as necessary to fulfill a legitimate business need. The more sensitive the data, the stronger the protections should be. We have seen positive movement in this direction with the major search engines, for example. They are now involved in a privacy arms race – each trying to retain consumer data for less time than the others.

Third, companies that materially change their privacy policies should explain those changes to consumers who have agreed to let their data be collected, and allow them to choose whether they want to continue under the new terms.

And fourth, companies that use sensitive data in advertising should collect it only after getting affirmative express consent from consumers to receive such advertising. Health records, financial information, Social Security numbers, home addresses, anything at all about children – these certainly comprise sensitive data. And in the gray areas beyond that, if you want to continue to self-regulate, you will need to be – well – sensitive to what others consider sensitive personal information.

Of course, the world of Internet advertising is dynamic – just look at the growth of Twitter or Facebook – or the competition between the likes of Apple and Google to buy mobile advertising companies. For that reason, we’ve continued to follow up in this area. After a recent series of roundtables exploring privacy and new technologies, we expect to issue guidance that addresses broader Internet privacy issues beyond behavioral advertising.

You will have to stay tuned for our broader privacy guidance. In the meantime, you really can’t go wrong if you just follow the simple principle of allowing truly informed consumer consent and consumer control to rule cyberspace. In this case, doing what is right – respecting your customers’ most basic rights to privacy and well-informed choice – is also doing what is good – good for business, good for consumers, and good for the growth of an ever-expanding, innovating cyberworld.

Finally, before I turn this discussion over to the panel of experts who are going to explain exactly how we will achieve all this, let me say a brief word about educating our children about Internet safety and another brief word about net neutrality.

I want to give a plug for the FTC’s latest consumer education piece, *Net Cetera*.² We brought copies here so that any of you who are interested can pick up a copy on your way out.

We developed this guide to help parents talk to their children about how to use the Internet safely, and it covers topics like cyberbullying and social networking. We’ve been partnering with schools and community groups to distribute it – over 2.5 million copies so far. We hope that some of you might see fit to distribute it to your Internet customers. You can print out copies or place bulk orders for booklets on the ftc.gov website. We think it would be a terrific complement to industry education efforts like the PointSmartClickSafe.org website.

With regard to net neutrality, I am on record supporting some form of non-discrimination requirement for ISPs. And this is not because I believe the cable industry wants to pick and choose what sort of content its customers receive. In fact, as I think I’ve made clear, I credit you with helping to lead us into a world where our communication, entertainment, education, and business choices are almost unlimited.

But I do believe that we need to retain the open character of the Internet that has led to so many of the innovations that make your broadband services something that consumers want to buy. Moreover, the firms that invest so much in the Internet, like all of you here today, will benefit from clear rules of the road on net neutrality far more than you will suffer from any set of rules the FCC promulgates.

Indeed, you – the broadband cable industry – have said that you don’t discriminate against certain content or applications on the Internet. I take you at your word. And that word – combined with the paucity of obvious net neutrality violations to date – begs the question: Isn’t the rhetoric on both sides a little overheated?

² *Net Cetera: Chatting With Kids About Being Online*, available at <http://www.onguardonline.gov/pdf/tec04.pdf>.

I believe my friend Julius Genachowski, who is speaking here tomorrow, has done a balanced job taking on this issue – rejecting both extremes and working openly with every stakeholder (unlike some previous FCC chairs). As a competition and consumer protection agency, we're going to stay active in this area. But I support everything Chairman Genachowski is attempting to do.

And now, I want to end where I started: Thank you. Thank you for letting a kid straight from the dentist make us laugh and a spinster from Scotland make us cry; for the Sopranos, foreign films on demand, and Top Chef; and for C-SPAN and C-SPAN radio, too. Thank you for opening the door to an unbelievable world of information and communication – and then letting us choose where to go. And thank you for your time today.