"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

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 …"

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