At the Intersection of Online Advertising and Privacy:
FTC Enforcement, Policy, and Encouragement of Self-Regulation
Remarks of FTC Chairman Jon Leibowitz as Prepared for Delivery
Ad:Tech NY
November 8, 2011

Thank you, Brad, for inviting me here today to speak, and to Warren Pickett, and the rest of your staff, who did a fabulous job putting this event together.

So, who's sticking around for the reception tonight? It's going to be held right in this room, and it should be a pretty good party.

And why wouldn't it be? We are in New York City, where Truman Capote held the Black and White Ball, dubbed "the party of the century" forty-five years ago almost to the day and just a few dozen blocks uptown from here. Where in the 1970s, my old neighbor John Travolta and friends danced the nights away at Studio 54. Where today, you can't walk a block without running into a celebrity headed for a Chelsea night spot or a crowd converging on an open air revel for Halloween, Fashion Week, or New Year's Eve in Times Square.

But none of this compares to the shindig the high tech advertising industry, with help from publishers and marketers, is throwing.

Thank you all for hosting a party in cyberspace. Your guests – consumers – are having the time of their lives, checking into cyberspace to do everything from diagnose their cat's skin condition to find their future spouse. And the economy, which, frankly, deserves a little fun after the last few years, is the belle of your ball: From 2000 to 2010, Internet advertising revenue increased from $8 billion to $26 billion. I think I just heard Ben Bernanke pop a bottle of champagne over in the VIP room.

What a cyber celebration – everyone's invited, the bar never closes, and the drinks are free.

Or are they?

As you well know, the advertising you create, to a great extent, is picking up the tab for all of this free online content we have come to expect and enjoy. And it is not just any sort of advertising but high tech, targeted marketing that relies on the collection, analysis, and storage of information about who consumers are, what they do, and where they go on the Internet – often without their knowledge or consent.

It is at this intersection of advertising online and privacy rights that the FTC jumps in, not to erect a stop light but to take a look at traffic patterns. Our mission is to safeguard consumer privacy – developing national policy, enforcing consumer protection laws and regulations, and educating businesses and individuals. But that is not all we do: We fight financial fraud, false advertising, and identity theft. On the antitrust side, we free the marketplace of anticompetitive conduct, review mergers, and challenge unfair business practices so that honest business people like you can continue to serve your customers and make a profit. As I told the Chamber of

Commerce earlier this year, we are an enforcement agency, not a regulator – and the FTC strives to keep burdens on businesses to a minimum.

Advertising has been an issue in the FTC's portfolio for more than half a century, and privacy for almost that long. More recently, we've looked at online behavioral advertising, data collection, and consumer tracking, which represent a market transaction of exactly the type that needs to be fair to all parties: Consumers online agree to give up some of what the father of the FTC, Justice Louis Brandeis, called the "right to be let alone," and in return, they get personalized advertising and an open invitation to the cyber-party of the 21st century.

Of course, we know that Americans expect a healthy dose of marketing with their entertainment: This is a nation that cheers the Allstate Sugar Bowl played at the Mercedes-Benz Superdome, buys car oil based on the patches on their favorite NASCAR driver's jumpsuit, and munches Reese's Pieces while watching E.T. phone home. Far more importantly, most consumers, including myself, appreciate viewing ads online that are customized to our interests: Who wants to scroll through a leggings' montage from Forever 21 when you can instead open your computer right to the announcement of LL Bean's annual chinos sale?

When consumers trade some of their privacy online for all the riches of cyberspace, we at the FTC are not interested in debating whether that is a good deal: we know the economy benefits and no one has complained to us that there is too much great free content online. We are more concerned that some consumers don't even know that they have made a deal at all – or if they do, they don't understand the price they are paying.

Last month, we coined the term "cyberazzi" to explain how online tracking works. Like the paparazzi who follow celebrities, online cookies and other data catchers follow consumers as they browse, reporting their every stop and action to many of you in this room who, in turn, collect an astonishingly complete profile of consumer behavior online.

Of course, every click on the Internet is not the sound of the cyberazzi shutter. But that still leaves too many consumers who do not understand they are trading their privacy for free online content or who have not made an informed choice to do so.

And even if they have, they may not know or accept that they often lose control over their personal data once it is captured. A consumer who has no problem revealing her browsing history to advertising companies targeting their pitches to her interests may feel very differently about the collection of that information if it's going to the financial company deciding whether to give her a mortgage, or the health insurer setting her rates, or the prospective employer determining her career path. I'm sure most of you would agree that all of us ought to have control over how data about our browsing habits are used. To its credit, the online advertising self-regulatory program run by the Digital Advertising Alliance announced some changes yesterday that address these concerns.

As you know, we have proposed a "Do Not Track" option that would allow consumers to choose whether companies can collect data about their online searching and browsing activities. To be effective, such an opt-out system would contain several elements.

It should be universal, honored by not just the advertising industry, but also by other companies that track consumers online. Consumers would have to be able to find and use the system easily and the tracking preference should be persistent – it shouldn't disappear if a consumer clears her cookies or updates her browser. And most important, Do Not Track should allow consumers to do more than just turn off targeted advertising; they must be able to opt out of the collection of behavioral data for all purposes except for a few specific categories like preventing click fraud and facilitating billing.

Our vision of Do Not Track bears some similarities to the successful Do Not Call program. Now with more than 200 million registered phone numbers, Do Not Call has brought peace and quiet to Americans' dinner hour; no wonder Dave Barry called it the most popular government program since the Elvis stamp. But unlike Do Not Call, we do not think Do Not Track should be administered by the government. We hope instead that you in the industry will work collaboratively to give consumers choices about how and when they are tracked online.

As many of you are aware, the Digital Advertising Alliance, which is composed of advertising trade associations, is making progress on its "Ad Choices" program, which allows consumers to opt out of targeted advertising. While the DAA's system is not yet universal, it is doing a nice job expanding throughout the galaxy: Many in this room – advertisers, advertising networks, and brands – have joined in this significant and impressive effort. Those of you who haven't: think about doing so. Unless those other companies also participate in offering meaningful choices about online tracking, the few party poopers who don't are going to make the system much less effective.

The DAA's ad icon is popping up in more and more places, but some work needs to be done to make the choices it offers easier to understand and exercise. We don't want DAA's Ad Choices to follow the model of mortgage disclosures, confusing lots of information with useful information.

We are also encouraging the industry to ensure that consumers get to choose not just the advertising they see, but also the information about them that the advertisers – and others – collect. In other words, consumers should decide not just what they watch, but whether and how much they are watched.

And finally, we are heartened to see the DAA working with the BBB to establish an enforcement program. Not every self-regulatory program includes real accountability, but the ones that do work better and generally are able to avoid a more regulatory heavy hand from Congress. This morning, the BBB announced six enforcement actions against online advertisers who agreed to follow the Online Interest-Based Advertising Accountability Program for not offering adequate opt-outs. That's a promising start.

We encourage the DAA to join with the browser companies to make the Ad Choices' opt-out permanent and move us closer to a Do Not Track architecture that is persistent. Microsoft, Mozilla, and Apple have implemented their own Do Not Track features, and about a half dozen advertising networks have pledged to honor the Mozilla Do Not Track header. We hope and expect that that is just the beginning of a groundswell.

The FTC staff, including our chief technologist, Ed Felten, a Princeton engineering professor, is involved in the W3C, a key Internet standards-setting body working on defining technical standards for Do Not Track. W3C has the participation of all interested stakeholders – advertising and technology companies (including the DAA), publishers, browser companies, and public interest groups. We think the group will strike a balance that provides effective choices but does not interfere with the normal data flows necessary for a thriving Internet.

We know you want to throw the sort of party that consumers clamor to attend. And as you continue to develop increasingly refined browser controls and more granular ad industry programs like the DAA system, implemented by companies like Evidon, consumers will choose to receive your targeted ads and agree to the tracking that backs them – because they will feel certain that the information they reveal will enhance and personalize their Internet experience, not harm or embarrass them. Online industry will flourish even more; in fact, statistics demonstrate that few consumers ultimately opt out when using the DAA mechanism.

Primarily because it makes good business sense, most companies, especially the ones in this room, will want a balanced, self-regulatory approach to Do Not Track. But some small faction will not, continuing to rely on cyberazzi to collect consumer data surreptitiously. These are the players who will keep the issue open in Congress and allow privacy advocates on both sides of the aisle to use the online advertising industry as an occasional piñata, rather than consistently commending you for the benefits you bring all Americans.

Of course, digital advertisers are not the only businesses that thrive on the Web or the only hosts of the cyber-party of the century. As with any really hot party, the room is full of models; that is, business models like behavioral advertising, but also ones like social networking, cloud computing, and mobile services and sales.

The FTC strives to keep up with the challenges of these ever expanding e-commerce and e-advertising markets. For example, next month we will host a privacy workshop to explore facial recognition technology and what it implies for privacy, security and Internet innovation. We hope to see many of you there, as this new technology is creeping into everything from online social networks to digital signs to mobile apps.

Our most ambitious effort along these lines was a December 2010 preliminary staff report on privacy that drew on roundtable discussions with a wide range of stakeholders. In it, we proposed a new framework for safeguarding consumers' personal data, one flexible enough to allow both businesses and consumers to continue to profit from an innovating, growing, and rich information marketplace.

We expect to issue a final report in the coming months. And we expect it to be complementary with the important work the Department of Commerce is doing on privacy.

Our preliminary report puts forth three principles to guide policymakers and industry as they, we hope, work together to protect consumer privacy online.

First, privacy by design. Companies in the business of collecting and storing consumer data need to build privacy protections into their everyday business practices. The more sensitive the data, the stronger the protections should be.

Second, transparency. Companies that collect and maintain consumer data online, especially the data brokers, need to tell consumers what's going on – and allow them to choose whether they want their data collected for that purpose. And by this, I do not mean another three-point font, ten-page document written by corporate lawyers and buried deep within the site. Our staff has been looking at data disclosures on mobile devices; one form took 109 clicks to get through, and the staffer who discovered that is probably the only one who ever made it to click number 109. Don't try to read this policy while driving.

Transparency is not an unreasonable request. My daughters can go to any of a number of retail clothing websites, and, with one click, see a clear description of a pair of pants – color, sizes, fit, customer reviews, shipping options. One more click – that's a total of 2, not 109 – 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.

Third, choice. Consumers should have streamlined and effective choices about the collection and use of their data. Businesses shouldn't have to offer any choice when consumers expect data to be shared, for example, to fulfill a customer's order. Choice, of course, includes Do Not Track.

While we at the FTC are proud of our work on privacy policy, we do more than talk a good privacy game. We are primarily an enforcement agency, and over the last ten years, we've brought more than 100 spam and spyware cases, almost 80 Do Not Call cases, and 34 cases for inadequate data security – most of which ended in companies adopting comprehensive security programs and agreeing to undergo independent audits every year.

We have also brought cases against powerful online companies: Google for using Gmail contact information to start up its Buzz social network without consumer consent and Twitter for data security lapses that allowed hackers to gain control of accounts – one sending tweets purportedly from President Obama offering the chance to win $500 in free gas.

While Google and Twitter are household names, the online advertising industry may be a bit of a mystery to the average consumer. But it's not to the FTC. When we see a violation, we take action. Last spring, we wrapped up a major enforcement effort aimed at the online advertising network Chitika, which we alleged violated the FTC Act by offering consumers the ability to opt out of targeted advertising – but without telling them that the opt-out lasted only ten days.

That is not only wrong, it is unacceptable: Consumers deserve meaningful – not illusory – control over what companies do with their personal information. Chitika agreed to a 20-year order that prohibits future misrepresentations, requires links to an opt out that is effective for at least five years on all of its ads, and requires the company to destroy personal data collected while operating with the vanishing opt-out.

Just today we announced another behavioral advertising case against ScanScout, which involves flash cookies. ScanScout is the Web's largest video in-stream ad network. The company's privacy policy stated that consumers could stop ScanScout from tracking them by

deleting cookies through their browser. However, ScanScout used flash cookies, which are not affected when consumers try to delete them. The final order requires ScanScout to place a tracking opt-out on their home page and in advertisements – one that is easy for consumers to find, understand, and use.

These cases – the first of many more major privacy enforcement cases you'll see from us – should send a signal: the FTC will not tolerate attempts to undermine consumer choice.

I got an email from the conference organizers last week giving me the "411 on all the ad:tech parties" this week. It said, and I quote, "One thing is for certain, the digital marketing industry definitely loves to party."

But we already knew that, didn't we?

Because you really are throwing the cyber-party of the century. And we at the FTC have no interest in shutting it down. On the contrary, we are all enthusiastic guests, playing Angry Birds and following Lady Gaga's tweets along with everyone else. More important, you are helping us do our job, opening new markets and opportunities for consumers, keeping the economy growing and innovating in trying times. Our only concern is making sure that all your guests understand there could be a cover charge; when there is, they should get to make meaningful choices about how much they are willing to pay to get in. But beyond that, in the immortal words of the B-52s, "let's keep this party going."

Thank you and I would be happy to answer questions.