The FTC's Consumer Protection Program:
Current Priorities In Advertising and Privacy

Jessica Rich, Federal Trade Commission
Kelley Drye & Warren Privacy and Advertising Law Summit
June 12, 2014

Good morning. I am delighted to be here to talk about the FTC's work and priorities in advertising and privacy.

And I'm doubly delighted to be here with Jodie [Bernstein], the greatest Bureau Director ever, and my mentor since my early days at the FTC. As you may recall, Jodie launched many of the programs that define the FTC today – our privacy program, the FTC's workshops and fraud sweeps, and our signature consumer and business education, among many other things.

The agenda for today's summit is an ambitious one, addressing advertising and privacy, and I know you'll be hearing from a number of my colleagues later today. To set the stage for today's discussion, I'll provide an overview of the FTC's activities and priorities in these areas. Hopefully, we'll have some time for some questions at the end.

As background, and as I think as many of you know, the FTC's primary authority comes from Section 5 of the FTC Act, which prohibits unfair and deceptive practices. We have used this law for decades to challenge a range of practices, including those involving advertising and privacy.

Additionally, under Section 12 of the FTC Act, we have authority to prohibit the false advertising of foods, drugs, devices, cosmetics, and services. Section 5 and 12 together give the FTC the power to ensure that advertisements promoting products are

truthful and not misleading and that objective claims are substantiated before they are made.

Advertising

Let me address advertising first. Our primary focus in this area is on deceptive ads that put consumers' health and well-being at risk. And we often focus on stopping deception that we see repeatedly in the marketplace, to prevent it from becoming even more widespread.

Our key areas of focus include disease claims, weight loss, disclosure issues, and cognitive products. I'll also briefly address native advertising and substantiation this morning.

The first area is **disease claims**. We have serious and continued concerns about dietary supplements and foods making disease claims without adequate substantiation. Our case against POM Wonderful is a good example. POM claimed that its juice products could treat, prevent, or reduce the risk of heart disease, prostate cancer, and erectile dysfunction, and that they were clinically proven to work. The Commission unanimously found that POM's disease claims were not substantiated and that its products were not clinically proven to work. When consumers drink juice or take a pill or powder to treat or prevent a disease, and those substances haven't been shown to be effective, consumers may be forgoing other treatment or diet and lifestyle changes and creating serious risks to their health. The Commission takes these claims very seriously and has made them a priority.

The second and related area of focus is **weight loss**. You may have seen our sweep in January against Sensa, L'Occitane, LeanSpa, and HCG Diet Direct. We alleged that these companies engaged in classic deception about weight loss and body slimming, and we hope that the sweep was an important reminder to companies about the consequences of doing that.

Sensa said you could sprinkle a powder on your food and lose substantial weight – 30 pounds in 6 months – without diet or exercise. L'Occitane said that its skin creams could trim 1.3 inches off a user's thighs in 4 weeks, just from rubbing it on. HCG Diet Direct said its hormone product was a weight loss miracle that would enable consumers to lose 40 pounds in 40 days – granted, the company encouraged people to diet too, but at such a low caloric intake that it put consumers' health at risk. And LeanSpa said users of its supplements would lose 25 pounds in 4 weeks, again without diet and exercise.

These companies paid a total of $34 million dollars to resolve the FTC's allegations. And they're now under permanent orders banning the deceptive claims and requiring substantiation for future weight loss claims, including claims about having scientific proof.

In conjunction with announcing these cases, we also announced the release of an online guide for the media, called "Gut Check." This is an educational brochure, listing seven weight loss claims that are *always false*, explaining why, and listing possible examples of those claims. We are urging the media, on a voluntary basis, not to accept ads that make any of the seven false claims or that contain other obvious hallmarks of deception.

A third area of concern is **disclosures** – when they are needed and how to ensure that they are effective. Last year, we issued an updated version to our Dot Com Disclosures guide to provide specific guidance for making disclosures on mobile devices, Twitter, and other new media. In addition, our updated *Endorsement Guides* no longer encourage you to just say, regarding an endorser's statement that he/she obtained a certain result, "results not typical." To avoid deception, you need to disclose clearly and conspicuously the generally expected results.

Companies and their endorsers also need to disclose if they are being compensated for providing the endorsements. Our recent case against ADT, the home security company, was all about that. And in the case we just filed against NPB Advertising for false weight loss claims regarding their green coffee supplement, we also charged the defendants with failing to disclose that consumers who endorsed the supplement had received it for free and were paid to provide video testimonials.

Another FTC priority area is **cognitive products**, for consumers of all ages. This past Monday, the Commission voted to accept for public comment a proposed consent order against i-Health, the marketers of BrainStrong Adult, a dietary supplement containing the fatty acid DHA. According to our complaint, the companies claimed that their product is clinically shown to improve memory and helps prevent normal cognitive decline as we age. In fact, we alleged, their substantiation only tested certain types of memory and even then, yielded small, inconclusive results. And their study did not even measure cognitive decline.

The i-Health case is interesting because the companies funded and presented as substantiation a study in a peer-reviewed journal that supposedly supported their claims. But we alleged that the results of the study did not match the claims they were making. As in all of our cases, we looked at whether the advertising claims match the underlying substantiation. And we consulted with scientific experts in the relevant field to answer that question. Here, the claims and substantiation did not line up.

We're also concerned about false or unsubstantiated claims about the purported benefits of DHA for children. Last year the FTC issued refunds to consumers who'd purchased children's multivitamins marketed with false or misleading claims about the amount of DHA and the purported benefits for healthy brain and eye development. And in another case involving cognitive products, we have ongoing litigation related to claims by a company that its videos and flashcards can teach kids as young as nine months old to read.

Finally, the Commission has focused on issues surrounding **native advertising.** Native advertising blurs the lines between ads and content or editorials. We had a workshop in December to discuss these issues and get input from stakeholders. The basic principle that advertising sales pitches should be identifiable as advertising is not that difficult. What's trickier is determining what is adequate to identify or disclose to consumers that the article or story is in fact advertising. We are considering options, such as a report including guidance on native advertising.

In the meantime, we are continuing to address blatant deception involving the portrayal of advertising as content. For example, in our case against NBP Advertising,

the Defendants made many of their claims on websites set up to look like legitimate news sites, featuring mastheads of fictitious news organizations such as Women's Health Journal and Healthy Living Reviewed, as well as logos they appropriated from actual news organizations, like CNN and MSNBC. We didn't just challenge the deceptive claims about the products being sold; we also challenged the false depiction of the advertising as news content.

Before leaving the topic of advertising, I also want to address **substantiation**. Contrary to some of the talk we're hearing, the Commission's substantiation standard hasn't changed. The discussion has simply been about the level of substantiation included in our orders as "fencing in" for previous law violations.

Let me address first our substantiation standards absent an order. First and foremost, companies need to have at least the level of scientific support claimed in their advertising. So, if their ads claim that a product's health benefits are scientifically proven – a so-called "establishment claim" – they must have proof sufficient to satisfy that claim. For health benefit claims, often this will be one or more randomized controlled trials (RCTs) on humans, as shown in both the POM and i-Health cases.

For claims about a health product's efficacy that do not refer to a specific level of proof, advertisers must have a "reasonable basis," which we determine using the factors set forth in the *Pfizer* case. Generally, the standard is "competent and reliable scientific evidence," which consists of the type and quantity of evidence that experts in the field generally require for the claim at issue. For many of the efficacy claims in the health area, experts would require human clinical testing, just as with establishment claims.

As to the substantiation required in our orders, this has always been determined on a case by case basis, depending on the nature of the claims, the conduct, the costs and availability of testing, and other factors. This case-by-case approach remains unchanged, but I'd like to provide some general guidance about how the Commission is likely to approach this issue in health and weight loss cases:

First, you should expect our orders to continue to require at least two RCTs in weight loss cases or in cases where we have reason to believe that the company's substantiation was the product of fraudulent or unethical scientific conduct.

In other health cases where experts would expect RCT evidence, our orders generally will define competent and reliable scientific evidence as consisting of "human clinical testing," without specifying a required number of RCTs. This approach – illustrated in the i-Health order – clarifies that, under our substantiation analysis, we assess not only the quantity of evidence, but also the quality of that evidence and how it relates to the entire body of relevant and reliable scientific evidence.

There is one other feature of the i-Health order that I want to highlight. The order includes a provision that requires respondents to preserve and produce supporting data and documents for human clinical trials that they or their supplier conducted or sponsored. You should expect to see this provision in future orders. We have found that study write-ups sometimes contain conflicting statements or statements that don't match the underlying data, so having access to the data may be important in evaluating a company's substantiation. This requirement does not apply if a company relies on a

study reported in a peer-reviewed journal, and the report provides sufficient information to enable experts to assess the study's reliability.

Privacy

Now I want to turn to the issue of privacy and discuss the FTC's recent initiatives and current priorities. This area is near and dear to me, having worked on privacy and data security issues since the 90s, when the FTC first launched its privacy program. Since then, there have been enormous changes in the marketplace and in the scope and complexity of the issues surrounding privacy.

The most obvious changes, of course, are the changes in technology. We launched the privacy program at the dawn of the Internet age, to address the new challenges raised by the interactive nature of the medium, which allowed for instant collection and sharing of consumer data. Privacy was seen as important issue for businesses too, if they wanted to ensure the health and survival of the Internet as a commercial medium.

But now, consumers carry mobile devices with them wherever they go. Our movements are tracked in stores and in malls, through our mobile devices and through facial recognition technology. When we use devices to track our exercise, that data may be shared with companies we don't know. Mobile apps not only help us with directions and let us play games, but may also collect our location information and share it with third parties. We update our social network page with details about our whereabouts and preferences multiple times a day. And we are entering the age of the Internet of Things, with smart cars collecting data about our routes and our preferences, and appliances anticipating our consumption needs.

Clearly, these developments provide tremendous benefits that consumers want and enjoy. However, they also present enormous privacy challenges.

First, data collection has exploded – it's simply everywhere you go, and technology enables companies to store much more data for longer, which raises obvious privacy and data security risks.

Second, as ubiquitous as data collection is, it's often quite invisible. Many of our bedrock privacy principles – such as notice and choice – are based on the notion that a consumer interacts with the companies that collect their data. But today, many companies that collect consumer data – advertising companies, data brokers, all sort of middlemen – operate behind the scenes, invisible to consumers.

Third, with so many companies obtaining consumers' data, with screens getting smaller and smaller, and with privacy policies having become impenetrable legalese, it's virtually impossible for consumers who want to protect their privacy to do so.

And fourth, with all the high profile breaches we have been seeing in the marketplace, and the debates surrounding government collection of data, consumers have much greater awareness and concern about privacy than ever before. Consumers care about privacy, and companies ignore it at their commercial – and not just legal – peril.

I. The FTC's Privacy Priorities

Our current privacy agenda focuses on three themes that reflect the challenges that consumers and companies face today: Big Data, Mobile and Connected Devices, and Safeguarding Sensitive Data. These priorities are in many ways overlapping, but I'll take them one-by-one.

Big Data

First is Big Data. Big Data can of course drive valuable innovation – for example, it can be used to determine what medical treatments are most effective across a large population. However, it also raises obvious risks for consumers – virtually unlimited data collection without their knowledge or consent; data breaches involving this treasure trove of information; the risk that data will be obtained by identity thieves; and the concern that companies will make inferences about consumers that simply aren't true.

Our activities on the Big Data front include the recent release of a report on data brokers. The report is the result of a study the FTC conducted of nine data brokers, representing a cross-section of the industry. Our report found that data brokers collect and combine data from multiple sources and develop detailed profiles for sale to other companies – marketers, advertising companies, insurance companies, lenders, retailers, and telecoms – for use in marketing, fraud prevention, and searching for people. This typically happens behind the scenes, without any consumer knowledge or awareness.

And data brokers don't just collect and share raw data, they develop inferences about people and put them into categories – for example, Urban Scramble and Mobile Mixers, which characterize low income, minority consumers; Thrifty Elders; Financially Challenged; Bible Lifestyle; Leans Left, and many other such categories.

Although data broker practices clearly benefit consumers by helping them find and enjoy the products and services they prefer, they also raise concerns about the visibility of these practices and how this data is used. Our report therefore encouraged Congress to consider enacting legislation that would enable consumers to learn of the

existence and activities of data brokers and have some control over how the data is used – through opt-out or rights to correct data, depending on the type of data broker product.

But we're not waiting for Congress to pass a new law. We're also using our existing authority to address troubling data broker practices. One of the most valuable of these tools is the Fair Credit Reporting Act, which sets forth procedures governing some of the most important uses of Big Data – determining whether to give consumers credit, a job, or insurance. Earlier this year, for example, we announced settlements with two companies that advise merchants on whether to accept consumers' checks, based on their financial history. The complaints alleged that TeleCheck and Certegy failed to have appropriate procedures to maintain the accuracy of consumers' data and correct errors – failures that can cause consumers to be denied the ability to write checks. The companies each paid a $3.5 million civil penalty to settle the charges.

And we've brought similar cases recently against data brokers Spokeo, Instant Checkmate, InfoTrack, and Filiquarian for failing to provide reasonable accuracy for the data they provided to employers, and to assure that purchasers of the data would use it for purposes allowed under the FCRA.

In addition, we have hosted a series of workshops to start a dialogue on several trends in Big Data and their impact on consumer privacy. We held the first one last December, focused on the Internet of Things. We also held our Spring Seminar Series to address emerging products and services such as mobile device tracking in retail stores, the use of alternative scoring models to help companies predict consumer behavior, and data collection by health apps and devices used by consumers to manage their health

data. We plan to issue reports on all of these workshops, discussing the findings and best practices for addressing the privacy concerns raised.

In addition, this fall, we are hosting a workshop to explore the use of Big Data and its impact on American consumers, specifically low-income and underserved consumers.

Mobile Technologies and Connected Devices

A second area of focus is mobile technologies and connected devices. Over the last few years, this area has become one of the main priorities for the Commission – in privacy and more generally.

Clearly, the marketplace is moving to mobile, and consumer protections need to move with it. But it's not just "old wine in new bottles." Mobile technologies also raise special consumer protection challenges, due to the always-with-you, always-on nature of mobile devices; the ability of these devices to track your location and connect to each other; and of course the small screen or, increasingly, no screen.

On the policy front, the FTC has already issued several reports about kids' apps, mobile privacy disclosures, and mobile payments. We also hosted a workshop on mobile security last year. Our kids' apps reports showed that most of the apps surveyed collected personal information from kids' devices, and shared it with third parties. The information included unique device ID, precise geolocation, and telephone number.

We've also brought law enforcement actions challenging violations occurring in the mobile ecosystem. For example, last month we announced a settlement with mobile messaging app Snapchat for misrepresentations to consumers about the disappearing nature of the photo and video messages sent through its service. We also settled a case

against the maker of a popular app that allows consumers to use their mobile devices as flashlights. We alleged that the app promised it would collect data from users' devices for certain internal housekeeping purposes, but failed to disclose that the app transmitted the device's location and device ID to third parties, including mobile ad networks.

In addition, we brought a series of cases this past year against Aaron's rent-to-own stores for installing invisible tracking software on rented computers that captured consumers' keystrokes, location, and account information and emails, and even took pictures of them in their homes. We also challenged the data security practices of web camera company, TRENDnet, whose poor security procedures allowed hackers to access live feeds of what was happening in consumers' homes.

Safeguarding Sensitive Data

A third area of focus is providing strong safeguards for sensitive information – that is, kids', health, financial, and precise geolocation data.

Protecting sensitive data isn't really a new priority – it's one of those bedrock privacy principles that will be here forever. But the changes I've been talking about – the ubiquitous and invisible data collection that takes place all day long – raise the stakes for sensitive data as more and more kids have smartphones, and data is collected from consumers through their health devices, their flashlights, their cars, and in so many other unexpected ways.

Our work to protect sensitive data includes over 50 settlements we've obtained against companies that failed to implement reasonable security protections – including companies such as Microsoft, DSW, TJX, Lifelock, CVS, and Rite Aid. Many of these

cases involve, not just consumers' financial data, but also their sensitive health information. One of our earliest cases – against data broker ChoicePoint – may be the best known. In that case, the company sold data to identity thieves despite obvious red flags, such as the fact that the thieves submitted multiple applications from supposedly different businesses from a single fax machine at a Kinkos copy store.

In addition, while we continue to use our existing authority to protect consumers' sensitive data, the Commission also supports new federal legislation to enhance our authority in this area. The Commission believes that a new federal law making clear that all companies must secure their data, and providing civil penalties for violations, is critical to change the incentives and provide appropriate deterrence in this area.

Finally, last year, we also updated our Childrens Online Privacy Protection Rule to address the increasing use by kids of interactive technologies, including mobile devices and social networks, and provide greater flexibility to companies obtaining parental consent.

Conclusion

This was just a brief overview of "where we have been and where we are going" in our privacy and advertising programs. Thank you again for having me. I'm happy to answer questions.