Federal Trade Commission

Consumer Protection 2016.0: Challenges in Advertising

Jessica Rich[1]
Director, Bureau of Consumer Protection, FTC

Association of National Advertisers – April 7, 2016

Good morning. I'm delighted to be here. I don't have to tell anyone in this room that your industry is in the midst of a technological revolution. Digital marketing and consumer data are overtaking the era of TV, print, and radio advertising. From Facebook to YouTube, from text messages to tweets, timing and context are everything. Brands are looking to connect with the right consumer at just the right moment. To do that, they rely on a high-tech, personalized experience – one that uses detailed data about who consumers are, what they do, and where they go, to make predictions about their likely behavior.

There's no question that consumers have benefitted enormously from this explosive growth. Every day, we encounter new products and services once left only to the imagination – smart cars, smart homes, wearables, smartTVs, everything you can think of. Personalization can save us time and provide other conveniences. And for businesses, there are many new opportunities for innovative and cost-effective advertising.

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

But these changes also pose immense challenges for consumer protection. Today, commerce comes at us from every direction, at every minute – through the smartphones we carry with us everywhere and the many connected devices all around us. Data-driven predictions determine the information we receive and the offers we get. And, increasingly, consumers become the marketers, as they're enlisted in campaigns on social media to tout products and services to their friends and acquaintances.

Adding to these challenges, many of the technologies that drive these advances now have small screens or no screens at all. And many of the companies that receive and use our personal information are behind the scenes, completely invisible to us. As a result, it's harder to rely on some of the traditional tools we've all used to protect consumers, such as disclosures to avoid deception and privacy policies to describe data practices. And it's extremely hard for consumers to protect themselves.

The FTC has made significant shifts in its consumer protection agenda to address these challenges. Today, I'm going to talk about the FTC's recent work to protect consumers from deceptive advertising and violations of their privacy. In both areas, the FTC's goal is to make clear that despite and amidst the vast changes we're seeing in the marketplace, the fundamental principles of consumer protection still apply: Tell the truth, the *full* truth. In your businesses decisions, weigh any harms you might impose on consumers very carefully. Don't help others deceive or harm consumers. These principles are timeless, and we expect companies to abide by them across all of their business models – old and new.

I. Deceptive Advertising

Let me start with the topic of deceptive advertising. The rise of mobile and other new platforms have provided a host of new ways to deliver advertising to consumers. To keep pace

with these developments, the FTC has spent significant resources developing our investigatory tools and bringing enforcement actions that involve new technologies. Today, I'll highlight three topics in particular – deceptive health claims, deceptive endorsements, and native advertising.

Deceptive health claims

Deceptive health and safety claims have been, and remain, one of the FTC's top enforcement priorities. These claims raise particular concerns because, if they're false, they can cause real harm to consumers. Thanks (or perhaps no thanks) to the smartphone explosion, we're seeing these type of deceptive claims all over the mobile platform.

The rules are pretty simple. Under the FTC Act, whether we're talking about traditional TV, magazine ads, tweets, texts, or websites, advertising must be truthful and not misleading. Advertisers also must have a *reasonable basis* for all advertising claims they make.[2] That means any claim – express or implied, made in ad copy or by a spokesperson or paid endorser – must be backed up by reliable evidence.

There's no end to the variety of deceptive health claims we're seeing. For example, we recently charged athletic apparel company Tommie Copper with making unsubstantiated claims that its copper-infused compression clothing would relieve severe and chronic pain and inflammation caused by arthritis and other diseases.[3] The company paid $1.35 million to settle the claims, and is potentially liable for much more.[4]

We also brought suit against Sunrise Nutraceuticals for making false and unsubstantiated claims that its supplement Elimondrol can treat and even cure people who are addicted to

[2] *Advertising Substantiation Policy Statement*, appended to *Thompson Medical Co.*, 104 F.T.C. 648, 839 (1984), *aff'd*, 791 F.2d 189 (D.C. Cir. 1986), *cert denied*, 479 U.S. 1086 (1987), *available at* https://www.ftc.gov/public-statements/1983/03/ftc-policy-statement-regarding-advertising-substantiation.

[3] Tommie *Copper Inc.*, No. 7:15-cv-09304-VB (S.D.N.Y. Dec. 2, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3194-x160007/tommie-copper.

[4] The order imposes an $86.8 million judgment against the defendants, which was partially suspended upon payment of $1.35 million by the defendants. If the defendants are found to have misrepresented their financial condition, the total amount will immediately come due.

opiates, including prescription pain medications and illegal drugs such as heroin.[5] This case is pending in federal district court.

And we're seeing more and more mobile apps marketed essentially as medical devices. Last year, we charged two app developers with deceptively claiming that their apps – Mole Detective and MelApp – could detect symptoms of melanoma, even in the early stages.[6] In fact, we alleged, the companies lacked evidence to show they could detect melanoma, early or at all.

One particularly troubling trend we're seeing involves deceptive health claims targeted at particular age groups. Many of these claims tout products offering cognitive benefits or other age-related treatments for older adults or young children – a clear effort to tap into the anxieties of aging baby boomers and those in the "sandwich generation."

For example, earlier this year, we charged the creators and marketers of the Lumosity "brain training" program with making unfounded claims that *Lumosity* games can help users perform better at work and in school, and could stave off memory loss, dementia, and even Alzheimer's disease.[7] As part of the settlement, Lumosity agreed to pay $2 million in redress and provide its subscribers with an easy way to cancel their auto-renewal to avoid future billing.

---

[5] F*TC v. Sunrise Nutraceuticals, LLC*, No. 9:15-cv-81567 (S.D. Fla. filed Nov. 17, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/152-3208/sunrise-nutraceuticals-llc.

[6] *Health Discovery Corp.*, No. C-4516 (Mar. 13, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3211/health-discovery-corporation-melapp-matter; *FTC v. New Consumer Solutions LLC et al.*, No. 15-C-1614 (N.D. Ill. filed Feb. 23, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3210/new-consumer-solutions-llc-mole-detective. *See also Koby Brown*, No. C-4337 (Oct. 25, 2011), *available at* https://www.ftc.gov/enforcement/cases-proceedings/102-3205/brown-koby-individually-dba-dermapps-et-al-matter; *Andrew N. Finkel*, No. C-4338 (Oct. 25, 2011), *available at* https://www.ftc.gov/enforcement/cases-proceedings/102-3206/finkel-andrew-n-individually.

[7] *FTC v. Lumos Labs, Inc. d/b/a Lumosity*, No. 3:16-cv-00001 (N.D. Cal. filed Jan. 5, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3212/lumos-labs-inc-lumosity-mobile-online-cognitive-game.

We also took action against Ultimeyes – another health app styled as a medical device – which claimed to have scientific proof that it could "turn back the clock" on consumers' vision through a series of visual exercises.[8] In fact, we charged it had no such proof.

The claims for children's products are just as bad. Last year, we took action against the makers of the *Jungle Rangers* computer game for claiming the game permanently improves children's focus, memory, behavior, and school performance – including for kids with ADHD.[9] It would be wonderful if a game could do that, but we alleged that the company's claims, again, were false and unsubstantiated.

Endorsements

The second area that I want to highlight is deceptive endorsements. Today, everyone's a salesman – the doctor on TV, the blogger you follow, your friends on Facebook. Given the ubiquity of reviews, blogs, and infomercials, we're seeing deceptive endorsements just about everywhere.

For decades, the Commission has made clear – through its cases and Endorsement Guides – that while testimonials and endorsements are a common and accepted form of marketing, there are certain rules you need to follow to make sure they're not deceptive. One is that if the person making the endorsement or testimonial has been paid or has other material connections to the advertiser, you need to disclose that fact. We recently updated the Endorsement Guides to address this principle, and many others, in newer forms of promotion like Twitter, affiliate marketing, "like" buttons, employee endorsements, and videos.[10] The guides lay out various

[8] *Carrot Neurotechnology, Inc.*, No. C-4567 (Feb. 23, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3132/carrot-neurotechnology-inc-matter-ultimeyes.
[9] *Focus Education, LLC*, No. C-4517 (Apr. 9, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3153/focus-education-llc-matter.
[10] *Endorsement Guides: What People Are Asking* (May 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/ftcs-endorsement-guides-what-people-are-asking.

advertising scenarios that are likely to deceive consumers, and provide guidance on ways to avoid this deception.

We're also challenging deceptive endorsements aggressively in our cases because, unfortunately, they're rampant. For example, last year, we took action against NourishLife for making unsubstantiated claims that it dietary supplement, Speak, was proven effective in treating childhood speech disorders, including those associated with autism. In that case, we alleged that the company not only posted a purportedly independent research site touting the supplement, but also featured endorsements from parents without disclosing that the parents were paid to make them.[11]

Also last year, we charged *Machinima*, an entertainment network that worked for Microsoft's ad agency, with paying a large group of "influencers" to develop and post videos online touting XboxOne. [12] The videos appeared to be the objective views of the influencers, and did not disclose that they were actually paid endorsements.

The governing principle is pretty simple: consumers have a right to know if a supposedly independent opinion is actually a marketing pitch. This is more important than even as consumers increasingly rely on reviews and blogs to make decisions about their purchasing and even issues like their health care.

Finally, in another important case last year involving consumer reviews, we charged that Roca Labs not only promoted unproven weight loss supplements, but also threatened to sue – and did sue – consumers who posted negative reviews online, thus preventing the truth about the

[11] *FTC v. NourishLife, LLC*, No. 1:15-cv-00093 (N.D. Ill. filed Jan. 7, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3152/nourishlife-llc. *See also FTC v. Lunada Biomedical, Inc.*, No. 2:15-cv-03380-MWF (PLAx) (C.D. Cal. filed May 12, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3067/lunada-biomedical-inc (alleging among other things that the supposedly independent bloggers recommending their supplements for weight loss and menopause symptoms were actually paid to do so).

[12] *Machinima, Inc.*, No. C-4569 (Mar. 17, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3090/machinima-inc-matter.

product from getting out.[13] The company had hidden a gag clause in the fine print of its terms and conditions but we charged that this type of gag clause was illegal.

Native Advertising

We have similar concerns about my next topic – native advertising – by which I mean the use of formats that make advertising or promotional messages look like objective content. The Commission recently issued an Enforcement Policy Statement and accompanying guidance on native advertising.[14] The policy statement explains how established truth-in-advertising principles apply to different ad formats, including native ads that look like surrounding non-advertising content. It affirms that ads and marketing messages that promote the benefits and attributes of goods and services should be identifiable as advertising to consumers.

The FTC also just brought a native advertising case against national retailer Lord & Taylor, our first such case following the policy statement.[15] We alleged that the company deceived consumers by paying for native ads, including a seemingly objective article in the online publication Nylon, without disclosing they were actually paid promotions for a 2015 clothing launch. The FTC also challenged the company's endorsement practices. We charged that as part of the clothing launch, the company paid 50 online fashion "influencers" to post Instagram pictures of themselves wearing a dress from the new collection, without disclosing it had given each influencer the dress and thousands of dollars.

The takeaway? When designing your marketing campaigns and hiring other companies to implement them, you must make clear that advertising is advertising.

---

[13] *FTC v. Roca Labs, Inc.*, No. 8:15-cv-02231-MSS-TBM (M.D. Fla. Sept. 28, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3255/roca-labs-inc.

[14] *See Commission Enforcement Policy Statement on Deceptively Formatted Advertisements* (Dec. 2015), *available at* https://www.ftc.gov/public-statements/2015/12/commission-enforcement-policy-statement-deceptively-formatted; *Native Advertising: A Guide for Businesses* (Dec. 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/native-advertising-guide-businesses.

[15] *Lord & Taylor, LLC*, Matter No. 152 3181 (Mar. 15, 2016) (proposed consent), *available at* https://www.ftc.gov/enforcement/cases-proceedings/152-3181/lord-taylor-llc-matter.

II. Consumer Privacy

Nowhere are the effects of technological change more dramatic than in consumer privacy. In recent years, data collection and use, personalization and predictions, and round-the-clock tracking have just exploded. Whether it's through a mobile device, Fitbit, smart car, social network, or thermostat, everyone is being tracked and profiled.

As I've emphasized, the use of consumer data can offer many benefits to consumers, including discounts, time savings, and even innovations that increase health, safety, and opportunity across large populations. But the privacy concerns are very real too. Do consumers know how their data is used? What would they think if they found out? Is the data being sold to companies that may misuse it? Is the data secure?

This is an important issue for businesses. Surveys increasingly show that consumers care about privacy, that it affects who they do business with, and that they are using their browsers and other tools to take steps to protect their privacy.[16] For example, we're seeing more and more consumers adopt ad blocking technology – which I imagine hurts the bottom lines of everyone in this room. One reason I think we're seeing this trend is because consumers haven't been provided with the choices they want when it comes to online advertising and tracking. They're using tools that are simple and available to take matters into their own hands. Consumer want, and are demanding, easy-to-use privacy tools, and industry can and must do a better job

[16] *See, e.g.*, Pew Research Center, *The State of Privacy in America: What We Learned* (Jan. 20, 2016), *available at* http://www.pewresearch.org/fact-tank/2016/01/20/the-state-of-privacy-in-america/; Morrison Foerster, *Consumer Outlooks on Privacy* (last visited Feb. 4, 2016), *available at* http://www.mofo.com/generalcontent/resources/mofoprivacyinsights (noting that more than one in three of the more than 900 U.S. consumers surveyed reported that they have elected not purchase products or services from a company because of concerns over what might happen with their data, and among those who identified themselves as being "concerned" about privacy, 82 percent identified privacy concerns as a factor that has adversely affected their decision to buy a product or service from a particular company); Pew Research Center, *Anonymity, Privacy, and Security Online* (Sept. 5, 2013), *available at* http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/ (finding that 86% of consumers have taken steps to remove or mask their digital footprints).

providing them, at their own peril. I'll have more to say about online tracking when I talk to the National Advertising Initiative next week.

Over the last two decades, the FTC has brought hundreds of privacy cases addressing a range of deceptive and unfair practices involving consumers' data – deceptive claims about how data is collected, used, and shared; failure to protect sensitive data from unauthorized access; invasive spam and spyware; the sale of sensitive data to scam artists; and the failure of seal programs to provide the promised protections. The companies we've sued have run the gamut, from retailers to data brokers, from tech companies to pharmacies, and from mobile apps to device manufacturers.

The FTC's central message, again, is that even in the face of rapidly changing technology and business models, companies still need to follow basic consumer protection principles. In privacy, these include: Don't collect or retain more data than you reasonably need. If you must collect data, de-identify it wherever possible. Protect data from unauthorized access. Give consumers accurate information and meaningful choices about their data.

We've emphasized these principles through enforcement, policy work, and education. Today, I'd like to highlight three topics: Data Security, Big Data, and the Internet of Things.

Data Security

In this era of data breaches, I don't need to tell you why data security is important. But I *do* want to emphasize that merely having a breach doesn't mean you've violated the law. The FTC recognizes that perfect security isn't possible, that the threats are constantly changing, and that hackers are now very sophisticated. The basic rule – and what the law requires – is that companies implement *reasonable* data security measures, taking into account the sensitivity and

volume of the consumer data they hold, the size and complexity of their operations, and the cost of available tools to secure the data.[17]

We've brought almost 60 data security cases to date, and many of the companies we've sued are household names. In no particular order, they include – *Eli Lilly*, *Guess Jeans*, *Petco*, *CVS*, *RiteAid*, *Dave and Busters*, *TJX*, *Life is Good*, *Fandang*o, *Microsoft*, *LifeLock*, *Oracle*, *ChoicePoint*, *LexisNexis*, *HTC*, *Wyndham Worldwide*, and *BJ's Warehouse*.[18] Most of these cases have involved the failure to address common, well-known vulnerabilities. For example, in *Wyndham*, we alleged that the hotel chain didn't require complex user IDs and passwords to access its systems, stored consumer data in clear text, and failed to take remedial steps even after a breach, resulting in two additional, similar breaches in rapid succession.[19]

Speaking of *Wyndham*, that case made big news last year because it was the vehicle for the Third Circuit affirming the FTC's authority to challenge companies' data security failures under the FTC Act. We felt confident we had this authority, but it's nice to have a circuit court agree. Despite our clear authority under current law, however, the FTC continues to support new data security legislation – to give the FTC additional tools to obtain civil penalties, to challenge data security failures by non-profits, to require breach notification, and to provide a level playing field for businesses.

A lot of our work in data security is educational – to stop breaches before they occur – and we have many materials on our website to help businesses develop a sound data security program. These include our recent guidance setting out the "lessons learned" from the FTC's

[17] *See, e.g., Commission Statement Marking the FTC's 50th Data Security Settlement*, Jan. 31, 2014, *available at* https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.
[18] *See generally* https://www.ftc.gov/datasecurity.
[19] *FTC v. Wyndham Worldwide Corporation et al.*, No. 2:13-CV-01887-ES-JAD (D.N.J. Dec. 11, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/1023142-x120032/wyndham-worldwide-corporation.

cases to date. I encourage all of you to take a look.[20] This past year, we've also taken our message on the road with our *Start with Security* campaign, which includes events around the country on security topics and best practices.[21] Our next *Start with Security* event will be on June 15, right here in Chicago.

Internet of Things

Next I'd like to turn to the Internet of Things. It *has* arrived. It's in our homes, our cars, and even on our bodies, and comes in the form of wearables, connected smoke detectors and light bulbs, and essentially any other Internet-connected device that isn't a mobile phone, tablet, or traditional computer. These products are innovative and exciting and provide real benefits. But they're also collecting, storing, and often sharing vast amounts of consumer data, some of it very personal, raising familiar privacy and security concerns and a bunch of new ones too.

One of the new concerns is device security and it's pretty serious. If hackers can hack your smart car, your pacemaker, or your insulin pump, you're really in trouble. And there's been evidence they can in some instances.

Our recent case against computer hardware company ASUS illustrates the problems created by poor device security.[22] Our complaint charged that critical security flaws in ASUS' routers put the home networks of hundreds of thousands of consumers at risk. We also alleged that the routers' insecure "cloud" services led to the compromise of thousands of consumers' connected storage devices, exposing their sensitive personal data on the internet.

---

[20] *Start with Security: A Guide for Business* (June 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business. *See also Protecting Personal Information: A Guide for Business* (Nov. 2011), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

[21] *See generally* FTC Press Release, *FTC Kicks Off "Start with Security" Business Education Initiative*, June 30, 2015, *available at* https://www.ftc.gov/news-events/press-releases/2015/06/ftc-kicks-start-security-business-education-initiative.

[22] *ASUSTeK Computer Inc.*, Matter No. 142 3156 (Feb. 23, 2016) (proposed consent), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3156/asustek-computer-inc-matter.

Also, we took action against TRENDnet, an Internet of Things company that sold IP cameras for home security and baby monitoring.[23] We alleged that, due to the company's failure to properly secure the cameras, hackers were able to access and then post online the private video and even audio feed of hundreds of people's bedrooms and babies' rooms.

The FTC also issued a report on the Internet of Things last year. The report recommended a number of best practices for companies to follow, and addressed how fundamental privacy principles can be adapted for the Internet of Things. For example, one issue we addressed was the question we hear again and again about whether notice and choice have continuing relevance in the IoT, given the lack of traditional screens or interface to communicate with consumers. Our answer was "yes," and the report discussed the different tools that IoT companies are using to communicate with consumers – such as point of sale disclosures, set-up wizards, or even codes on the device. The report also discussed the importance of reasonable collection limits, de-identification of data, and strong security measures. You can find the report online.[24]

Big Data

Finally, let me turn to Big Data, by which I mean the vast collection of detailed data about consumers to make predictions about populations or groups of consumers. Big Data can of course drive valuable innovations across society, but increased collection and storage of data also increases the risks of data breach, identity theft, and the likelihood that sensitive data will be used for purposes consumers don't anticipate or want – for example, by employers, insurers, and creditors to make decisions about consumers' eligibility for important benefits.

---

[23] *TRENDnet, Inc.*, No. C-4426 (Jan. 16, 2014), *available at* http://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter.

[24] FTC Staff Workshop Report, *The Internet of Things: Privacy and Security in a Connected World* (Jan. 2015), *available at* https://www.ftc.gov/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things.

We recently issued a report entitled *Big Data: A Tool for Inclusion or Exclusion?*[25] which followed up on a workshop we held. The workshop explored how the categorization of consumers may be both creating and limiting opportunities for them, with a focus on low income and underserved consumers.[26] A key message in our report is that there are laws currently on the books – including the Fair Credit Reporting Act, the Equal Credit Opportunity Act, and the FTC Act – that already address some of the concerns raised by Big Data. As you're creating and using Big Data, you must familiarize yourself with these laws, some of which are enforced by not just the FTC, but other agencies.

One theme I am stressing as part of the Big Data phenomenon is the connection between the sale of sensitive data and fraud. In fact, we often discover in our fraud cases that the scammers used highly sensitive information bought from another company, often a data broker – including Social Security and bank account numbers – to trick or steal from consumers.[27] This data goes well beyond the lead lists we've been seeing for years.

The FTC has brought a number of cases related to this growing problem. For example, in our actions against data brokers Leap Lab and Sequoia One, each company had been able to purchase the payday loan applications of financial strapped consumers – which included names, addresses, phone numbers, employers, SSNs, and bank account numbers – and then sell them to

---

[25] FTC Report, *Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues*, Jan. 2016), *available at* https://www.ftc.gov/reports/big-data-tool-inclusion-or-exclusion-understanding-issues-ftc-report.

[26] FTC Workshop, *Big Data: A Tool for Inclusion or Exclusion?*, Sept. 15, 2014, *available at* https://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion.

[27] For example, in our "phantom debt" cases involving the collection of "debts" from financial strapped consumers that the consumers did not actually owe, the defendants had purchased detailed information about the consumers from payday lending sites and other sources. *See, e.g., FTC v. K.I.P., LLC*, No. 1:15-cv-02985 (N.D. Ill. Apr. 6, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/152-3048/kip-llc-payday-loan-recovery-group; *FTC v. 4 Star Resolution, LLC*, No. 1:15-cv-0112-WMS (W.D.N.Y. Feb. 9, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3202/4-star-resolution-llc.

scam artists who used the data to withdraw millions of dollars from consumers' accounts.[28] Similarly, we've brought a number of cases against fraudulent debt collectors that were able to purchase detailed information about consumers' debts, including account numbers and SSNs. These types of cases reveal a very troubling trend and help to answer the question we so often hear in privacy – "where's the harm?" When you can simply purchase this kind of highly sensitive data about consumers' and use it to defraud them, there's harm.

III. Conclusion

In closing, I hope I've made my point that while the technological landscape is constantly changing, the basic principles of consumer protection are enduring and provide a solid and continuing framework for vigorous FTC enforcement. These principles aren't just about compliance, they're about your brand and consumer trust, so you have many reasons to care about them.

I also want to put in a plug for strong self-regulation, and for your cooperation with self-regulatory programs like the NAD. Self-regulation – and by that I mean strong, visible, and enforceable self-regulation that provides effective consumer protections – is an important complement to law enforcement, and helps the FTC maintain a safer marketplace for consumers and a level playing field for businesses. Thanks for having me here today.

[28] *FTC v. Sitesearch Corp., LLC*, Matter No. 142-3192 (D. Az. filed Dec. 22, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3192/sitesearch-corporation-doing-business-leaplab; *FTC v. Sequoia One, LLC*, No. 2:15-cv-01512-JCM-CWH (D. Nev. filed Aug. 12, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3253/sequoia-one-llc.