American Bar Association

What's In Store

What's In Store

Newsletter of the Section of Antitrust Law's Consumer Protection Committee, Privacy and Information Security Committee, and Advertising Disputes and Litigation Committee

Volume 25, No. 1, December 2016

Editors

Svetlana S. Gans
Federal Trade Commission
sgans@ftc.gov

Lydia Parnes
Wilson Sonsini Goodrich & Rosati
lparnes@wsgr.com

Terri J. Seligman
Frankfurt Kurnit Klein & Selz PC
tseligman@fkks.com

Patricia A. Conners
Office of the Attorney General of Florida
Trish.Conners@myfloridalegal.com

M. Sean Royall
Gibson, Dunn & Crutcher LLP
sroyall@gibsondunn.com

Ashley Rogers
Gibson, Dunn & Crutcher LLP
arogers@gibsondunn.com

What's In Store is published periodically by the American Bar Association Section of Antitrust Law's Consumer Protection Committee, Privacy and Information Security Committee, and Advertising Disputes and Litigation Committee.

The American Bar Association
Section of Antitrust Law
321 North Clark Street
Chicago, IL 60654

From the Editors

Welcome to the latest edition of What's In Store, which is chock full of information that you'll need to know as 2016 comes to a close.

We are pleased to include in this edition two interviews: one with FTC Commissioner Maureen K. Ohlhausen, and one with District of Columbia Attorney General Karl A. Racine. Commissioner Ohlhausen offers insight into the Commission's consumer protection priorities in 2017 and its key challenges moving forward as it continues to address consumer privacy and data security issues. She also discusses the effects of globalization on the Commission's consumer protection efforts, as well as her belief that the Commission should be allowed to bring its expertise to protect consumers from unfair or deceptive activities of common carriers and nonprofits. Attorney General Racine, who took office in early 2015 as the District of Columbia's first elected Attorney General, discusses his role in shaping that newly public-facing office. He also discusses establishing a new standalone Consumer Protection unit within his office and the new offices' priorities; the consumer protection-related trends he sees in the District of Columbia; and his consumer protection successes thus far. Finally, he discusses the unique relationship the District of Columbia has with the federal government, as well as he how he intends to tackle his next big challenges.

This edition also features an article by Ethan (Eitan) Levisohn, who provides an informative overview of the first enforcement action brought by the Consumer Financial Protection Bureau related to cybersecurity and data protection. Levisohn delves into the details of the Bureau's settlement, ultimately recommending that the time is now to make data security a "compliance priority."

Additionally, this issue includes a timely article by Dana Rosenfeld and Devon Winkles concerning the self-regulation of interest-based advertising and cross-device tracking technologies, which track and target users across multiple devices. Companies using these technologies should pay careful attention to this fulsome overview regarding the standards and enforcement programs of the organizations working to "balance the benefits of interest-based advertising with privacy concerns and creating frameworks for self-regulation."

Finally, we include an article by Katrina Robson, Hannah Chanoine, and Tristan Bufete, who analyze the FTC's approval in July 2016 of final consent orders against four companies that allegedly misrepresented their personal care products as "all natural" or "100 percent natural," despite the fact that the products contained synthetic ingredients. The authors caution that companies that improperly use modifiers like "100 percent" and "all" when promoting personal care products may very well face FTC scrutiny.

We welcome your feedback, and we encourage you to contact any of the editors to get involved in 2017.

IN THIS ISSUE

Q&A with FTC Commissioner Maureen K. Ohlhausen*

* The views expressed in this interview are solely those of Commissioner Ohlhausen and do not necessarily reflect the views of the Commission or any other Commissioner.

Maureen K. Ohlhausen was sworn in as a Commissioner of the Federal Trade Commission on April 4, 2012, to a term that expires in September 2018. Prior to joining the Commission, Ohlhausen was a partner at Wilkinson Barker Knauer, LLP, where she focused on FTC issues, including privacy, data protection, and cybersecurity. Ohlhausen previously served at the Commission for 11 years, most recently as Director of the Office of Policy Planning from 2004 to 2008, where she led the FTC's Internet Access Task Force. She was also Deputy Director of that office. From 1998 to 2001, Ohlhausen was an attorney advisor for former FTC Commissioner Orson Swindle, advising him on competition and consumer protection matters. She started at the FTC General Counsel's Office in 1997.

Before joining the FTC, Ohlhausen spent five years at the U.S. Court of Appeals for the D.C. Circuit, serving as a law clerk for Judge David B. Sentelle and as a staff attorney. Ohlhausen also clerked for Judge Robert Yock of the U.S. Court of Federal Claims from 1991 to 1992. Ohlhausen graduated with distinction from George Mason University School of Law in 1991 and graduated with honors from the University of Virginia in 1984.

Ohlhausen was on the adjunct faculty at George Mason University School of Law, where she taught privacy law and unfair trade practices. She served as a Senior Editor of the Antitrust Law Journal and a member of the American Bar Association Task Force on Competition and Public Policy. She has authored a variety of articles on competition law, privacy, and technology matters.

1. *What do you think the Commission's consumer protection priorities will be in the upcoming year, and what is driving those priorities?*

Though it doesn't always grab headlines, the Commission's bread and butter work is and should remain detecting and stopping fraud. Protecting all consumers from scams, particularly those that prey on the most vulnerable, should stay at the top of our list. The Commission has also long had a focus on rapidly changing technology and business models and that will continue. I think you are likely to see a renewed attention to enforcement where there has been real and substantial consumer injury. I expect the Commission will continue to focus on the value of information, and the benefits and challenges of big data will continue to be an important topic. Of course, the Commission will continue to seek to educate itself on new technologies and business models as they affect consumers.

2. *During your tenure as Commissioner, the FTC has done substantial work to address consumer privacy and data security issues. What are the Commission's key challenges as it continues to address these issues?*

I see three common pitfalls that are important to avoid in privacy and data security regulation—imposing the privacy preferences of a few on the many, focusing on hypothetical rather than real harms, and failing to treat similarly situated companies similarly. The Commission has generally, but not always, avoided these pitfalls.

We can avoid such pitfalls by maintaining what I call "regulatory humility." This includes respecting consumer autonomy and refraining from substituting the choices of regulators for those of consumers. Privacy is a great example. Consumers generally have similar privacy views about sensitive personally identifiable information (social security numbers, financial, health, information about children, and precise geolocation), but we know that they have widely varying privacy preferences about non-sensitive information. Keeping a targeted, restrained privacy approach will allow the Commission to protect consumers' privacy preferences without impeding innovation.

It is also vital to focus on actual or likely consumer harms, rather than hypothetical concerns. This directs the agency's limited resources to where they can benefit consumers the most. Identifying a concrete problem also allows the Commission to consider the proper tools for addressing the issue. Of course, we must consider how to minimize the costs and the unintended consequences of any action.

3. How has globalization affected the Commission's consumer protection efforts?

Globalization has increased the importance of inter-agency cooperation and interoperability in consumer protection, particularly with respect to data and privacy. The Internet has transformed how data moves, making cross-border data flow ubiquitous. This cross-border data flow has been a key driver of economic growth and international trade, but it also brings an increased need for interoperability and cooperation in enforcement.

The Commission has actively promoted cooperation and interoperability by engaging with over 100 foreign competition and consumer protection agencies and participating in several multinational privacy networks. We have successfully applied our data security and privacy laws to companies whose violations have international components and will continue efforts to promote interoperability with other nations.

One example of our ongoing efforts to promote privacy interoperability is Privacy Shield. The Commission will actively enforce the Privacy Shield framework and promote awareness of the framework among U.S. businesses and consumers. Additionally, the Commission will monitor implementation issues and work to improve the administration of the program.

Another example of the Commission's interoperability effort is the Asian-Pacific Economic Cooperation (APEC) framework. The Commission participated in APEC from the beginning, helping to develop the privacy framework, the Cross-Border Privacy Rules, and the Cross-Border Privacy Enforcement Arrangement. The United States was the first APEC economy to join the Cross Border Privacy Rules system, and the Commission was the first privacy enforcement agency the system approved.

These are just a few examples of our efforts to increase privacy interoperability. I'm confident the Commission will continue these efforts.

4. Is there any facet of consumer protection in which you believe the Commission should have more input?

The Commission should be allowed to bring its considerable expertise to protect consumers from unfair or deceptive activities of common carriers and nonprofits.

The common carrier exemption frustrates the FTC's consumer protection efforts with respect to a wide variety of activities—including privacy, data security, and billing practices—in the crucially important telecommunication and Internet industries. With the convergence of telecom, broadband, and other technologies, the repeal of the common carrier exemption makes sense. This is particularly true in light of the Ninth Circuit's recent decision in AT&T, which held the exemption extended to non-common carrier activities of common carriers. This means the FTC may no longer have jurisdiction to challenge deceptive and unfair practices related to cramming, deceptive marketing of internet services, the collection of children's information online, and unwanted robocalls. Allowing the FTC to act in this area and applying the same approach to all online participants would be in the best interest of consumers

Similarly, the nonprofit exemption to our jurisdiction hinders the Commission's ability to protect consumers. For example, despite many publicized data breaches at nonprofit hospitals and universities, the FTC cannot challenge unfair or deceptive data security or privacy practices of these entities. Further, while the Commission can use Section 5 to reach "sham" nonprofits, such as shell nonprofit corporations that actually operate for profit, satisfying this standard is resource-intensive. Removing the nonprofit exemption would enable

more efficient, effective application of our authority to the benefit of consumers.

Eight Questions for District of Columbia Attorney General Karl A. Racine

Attorney General Karl A. Racine brings over 25 years of experience as a practicing lawyer and good steward of leading law firms and organizations to the Office of the Attorney General. He has pledged to prioritize consumer protection, enforce affordable housing regulations, and find alternatives that can divert young people out of the juvenile justice system.

Attorney General Racine has deep and wide-ranging legal experience. He volunteered as a law student in a clinic supporting the rights of migrant farm workers; represented indigent residents in the D.C. Public Defender Service; practiced white-collar and commercial litigation with Cacheris & Treanor and Venable LLP; served as Associate White House Counsel in the Clinton Administration; and served on the District's Judicial Nomination Commission. At Venable, Attorney General Racine ultimately was named Managing Partner, overseeing 600 attorneys and becoming the first African-American managing partner at a top-100 law firm, The National Law Journal named him one of the 50 most influential minority lawyers in the United States.

A lifelong District resident, Attorney General Racine is deeply committed to the community, assembling what the Washington Post called "a rich record of community service." He remains involved in a variety of causes, including youth literacy and mentoring. Attorney General Racine earned his bachelor's degree at the University of Pennsylvania and his law degree from the University of Virginia School of Law.

1. You took office in early 2015 as the District's first elected Attorney General, and in your first year you opened a standalone Office of Consumer Protection. Why was it important for you to establish this new office as one of your early actions?

In 2010, the voters of the District of Columbia overwhelmingly voted to convert the then-subordinate Office of the Attorney General (OAG) to an independent office. Through this mandate, reflected in the subsequently passed legislation creating the office, the voters made clear that the new Attorney General had a responsibility to promote and defend the public interest for all D.C. residents. That law took effect in 2014, and the voters gave me the honor and responsibility of shaping this newly independent, newly public-facing office.

One of the best ways to ascertain the public interest is, of course, to listen closely to the public—something we set about doing very intentionally and comprehensively once I took office. Through community meetings, personal conversations, and phone communications to our office, it became clear that our residents were eager for more help in the area of consumer protection. This was especially true for vulnerable people who are often targeted by scammers—our seniors, low-income residents, members of our immigrant communities, and others.

With this community feedback and public interest mandate in mind, I established an Office of Consumer Protection (OCP) charged with zealously pursuing litigation, outreach, and education to protect consumers. That Office is now up, running and has become very active, both investigating matters locally and leading nationwide investigations along with other Attorneys' General Offices.

2. What were some of the Office of Consumer Protection's initial priorities?

I asked the OCP staff to focus on reaching out to, and undertaking enforcement actions on behalf of, consumers who were being taken advantage of—with a special focus on seniors, immigrants, low-income residents, and other vulnerable people.

OCP has done this by using its authority to conduct investigations and enforcement actions; increasing its community outreach; developing an extensive and growing library of educational materials on consumer-protection topics like Identity Theft, Student Loan Debt, and Financial Exploitation; and increasing our media outreach on consumer topics. The Office has also focused on increasing the public's awareness of the existence of our Consumer Protection Hotline and the newly available option of submitting consumer complaints, via e-mail and our

website, that are then mediated by our Ombudsman and investigators.

3. *What recent concerns in this area are you hearing from District consumers? Are there any trends you're seeing that we should be aware of nationally?*

The concern we hear consistently from residents in the District is the same concern that all consumers have: They think businesses should live up to their word and deal fairly with consumers, and they are upset when businesses don't deliver the services they've promised or deal dishonestly with consumers. While the specific issues we hear about may change from time to time—most recently, the hot issues have involved topics like student-loan debt, immigration-services fraud, and telephone scams—the principle stays the same.

With regard to recent national trends, consumer protection issues continue to arise around the "sharing economy." The sharing economy essentially allows companies to connect consumers to third parties, usually individuals, to perform some sort of service for them, utilizing either web platforms or peer-to-peer smartphone applications. These companies must typically abide by the same consumer protection laws as traditional businesses. One case we brought recently involved the popular sharing-economy company Handy Technologies (Handy), which we believe is unlawfully deceiving consumers.

Handy uses its website and a smartphone app to connect consumers with housecleaners. In its advertisements, the company used words like "trusted," "pre-screened," and "background-checked" to describe the housecleaners, but as our lawsuit alleges, Handy failed to properly screen for criminal histories. Ultimately, these housecleaners stole property from District residents. Additionally, Handy deceptively enrolled consumers who thought they were purchasing a one-time cleaning service into cleaning plans that billed them on a recurring basis.

Companies cannot skirt consumer protection laws simply because their business model is to serve as a conduit to connect consumers and independent workers. We must enforce and apply the law consistently to protect consumers even as technology changes.

4. *What's an example of one of your key consumer protection successes so far?*

One of the Office's first high profile cases was a suit against a Virginia-based couple who bought distressed properties in gentrifying parts of the District, then made money "flipping" them to buyers in our city's hot housing market. For multiple properties, these developers inadequately and improperly renovated the homes—often without proper permits and in violation of zoning laws. Once the homeowners uncovered the problems, they often found that their new homes needed tens of thousands of dollars or more in structural and other repairs simply to be brought up to code.

We coupled this litigation with community education and outreach about the warning signs residents should keep in mind when buying a home. Ultimately, the couple agreed to pay at least $1.6 million in restitution and costs, and they may no longer perform construction in the District without prior approval from our Office. Given the booming housing market in the District, we consider this not only a successful enforcement action, but also an important effort to raise industry standards through the successful resolution of a high-profile suit.

5. *While District of Columbia residents are continuing to push for statehood, the District is not a state and therefore has a unique relationship with the federal government. How does this relationship affect your consumer-protection efforts?*

Of course, the District suffers some disadvantages because we remain under the jurisdiction of Congress. But, being located in the city that is also the seat of the federal government does have some positive implications for our Office's consumer work. For instance, we have easy access to other consumer protection agencies and leaders, which allows us to build strong relationships, both formal and informal. These entities include federal agencies like the Consumer Financial Protection Bureau, the Federal Communications Commission, and the Federal Trade Commission, as well as advocacy and nonprofit groups like the Better Business Bureau and the AARP. Just living in the same metropolitan area as multiple national-level consumer experts, advocates, and regulators means we get to engage in a constant exchange of ideas and opportunities to collaborate. This helps us keep up to date on trends, news and best practices in a way that, I think, ultimately redounds to the benefit of District consumers, as well as consumers nationwide.

6. *Has your Office of Consumer Protection identified any legislative priorities that could positively impact consumers?*

Yes, our Office's newly gained independence allows us to introduce legislation for consideration before the D.C. Council (our equivalent of a state legislature). Because we receive consumer concerns from residents all across the District, we have a unique perspective that informs our legislative agenda and we have identified multiple areas where our laws need strengthening.

One piece of legislation we have introduced is the Immigration Services Protection Act of 2016. This bill combats "notario fraud," which targets immigrant communities. Notarios—Spanish for notaries public—are often known in Latin America as people who are authorized to practice certain types of law. While notaries public are not authorized to practice law in the United States, some still advertise themselves as able to offer legal advice and immigration services. Many non-citizens pay hundreds of dollars only to find out that they will never obtain a green card, legal immigration status, or other crucial benefits because they received incorrect advice from an unqualified notario fraudster.

We brought suit earlier this year against one such notario fraudster doing business in the District, but exploring the issues around notario fraud as we built our case made us realize the District's law could be improved to better protect consumers. This bill, which grew out of the work our Office does with the Council for Court Excellence and the Hispanic Bar Association of D.C., would give us greater tools to prevent such fraud.

7. *When a consumer protection issue arises, how does your Office balance the concerns of the business community with the swift action needed for consumers?*

First and foremost, our job is to enforce the laws of the District of Columbia—including our Consumer Protection Procedures Act. It is through this enforcement power and in service to our public-interest mandate that we work to protect the rights of D.C. residents.

But our aim is not to be confrontational for confrontation's sake. I understand that, when business and the public sector collaborate, we end up with better and more effective public policy. Our philosophy when it comes to consumer protection is to work in a cooperative and consultative manner with companies doing business in the District. While we will vigorously and aggressively prosecute bad actors who violate consumer-protection laws, we are also happy to meet with anyone from the business community to discuss concerns.

In addition to my open door policy, our Office has put together a Business Advisory Council to solicit

feedback from business leaders in the community. We encourage these leaders to educate us on the nature of their work in an attempt to avoid unnecessary burdens on business. This does not mean that we will always agree. However, I do believe that it is beneficial to understand any differences we may have, as well as provide a venue for businesses to proactively give input and have access to the OAG.

8. Looking forward, what's your next big challenge and how do you plan to meet it?

We often find that the consumers who suffer the most harm at the hands of bad actors are from vulnerable groups—and members of such groups are often reluctant to complain about such mistreatment to businesses or report it to authorities. As I mentioned earlier, we are currently fighting notario fraud targeting our immigrant communities. Unfortunately, immigration fraud like this can sometimes go unreported because victims are afraid to come forward due to their undocumented status or that of family members. Likewise, unscrupulous and abusive debt collectors often target vulnerable groups—and members of these groups often don't report it. We have taken aggressive action against multiple debt collectors for unlawful practices, such as harassing phone calls, usurious interest rates, and unlawfully transferring debt to third parties. For instance, last year we filed a complaint against CashCall, a debt-purchasing company that collects on consumer loans with interest rates often exceeding 300 percent annually. We also recently settled another suit against a debt collector, and we continue to investigate other debt collectors for unlawful practices.

These are prime examples of where community education is key; it's our job to inform the public that the Office of the Attorney General is here to protect all District residents and bring to justice those who would defraud consumers, including consumers in the immigrant community. In order to combat underreporting on the part of people who need us the most, we have to dedicate ourselves to deep and meaningful community engagement.

To that end, my colleagues and I have attended over 200 meetings in the past year at churches, senior centers, schools, community meetings, and more to educate the public and hear their concerns. We want District residents to know that our Office is here to help, regarding such issues as elder abuse, slum lords, human trafficking, mental health services, foreclosure issues, financial fraud, and much more.

Though our Office of Consumer Protection is off to a strong start with strong enforcement and community education initiatives, the one thing we encourage consumers to do to help us as we enter this new Office's second year is this: complain! Community engagement is a two-way street, and hearing from our District residents will help us better leverage the law to protect consumers.

The Consumer Financial Protection Bureau, Cybersecurity, and Data Protection

By Ethan (Eitan) Levisohn

Eitan Levisohn is an associate in the Washington, DC office of Jones Day. His practice is focused on advising banks and financial institutions on enforcement and regulatory matters before federal and state agencies. He has extensive experience investigating and litigating civil and criminal matters, including matters concerning the Dodd-Frank Act.

Before joining Jones Day, Eitan was one of the first dozen employees in the Office of Enforcement at the Consumer Financial Protection Bureau (CFPB), where he helped establish the Office and led investigations into potential violations of consumer financial protection laws, including UDAAP, the MAP Rule, and the FTC's Endorsement Guide. He also supported supervisory exams at the Bureau and gained experience in a wide range of consumer financial markets, including mortgage origination and advertising, mortgage servicing, deposit products, student lending, student loan servicing, and title insurance.

Prior to working at the CFPB, Eitan was a trial attorney at the Department of Justice in the Public Integrity Section, where he investigated and prosecuted public corruption and campaign finance matters.

In March 2016, the Consumer Financial Protection Bureau brought its first enforcement action dealing with cybersecurity and data protection.[1] The Bureau's involvement in the arena is not a surprise. Since its inception, the agency has aggressively asserted the breadth of its jurisdiction and made clear that it intends to actively participate in prominent consumer protection issues of the day, and there is almost no area that has a higher profile at the moment than data security. And while the Bureau has not yet brought additional data privacy actions, entities regulated by the Bureau should take note of the CFPB's activity and take the necessary steps to avoid being the subject of future supervisory or enforcement actions.

I. The Bureau's Dwolla Action

The Bureau entered a settlement with Dwolla, an online payments company, in March 2016. According to the consent order (which did not require Dwolla to admit the truth of the allegations), Dwolla promoted its services as generally safe and secure, and made specific representations that its data protection program was compliant with—and even exceeded— industry standards, that personal data was encrypted, and that mobile applications were secure. In fact, according to the CFPB, these claims were untrue and deceptive.

In the consent order, the CFPB alleged that Dwolla's procedures failed to meet industry standards, left personal data unencrypted, and allowed applications to be released without testing their security. Moreover, the CFPB's consent order more generally found that Dwolla, despite promises of safety and security, "failed to employ reasonable and appropriate measures to protect data obtained from consumers from unauthorized access," including appropriate policies governing the collection and storage of personal information, adequate risk assessments, and adequate employee training on data security. In the eyes of the CFPB, Dwolla failed to live up to both specific commitments and more general promises about security.

II. Lessons Learned

The CFPB's posture has conveyed the sense that this case was a relatively straightforward one, with an easy hook for the Bureau's assertion of data privacy jurisdiction. Dwolla made certain commitments to consumers which they are alleged to have failed to satisfy. On its face, it appears to be a textbook deception case, where a company overpromised and underperformed.

But looking deeper, this is not a classic consumer protection matter. First, there was no consumer harm alleged by the Bureau—while the failures identified by the Bureau were of the type that could, in the right circumstances, lead to harm, that risk never ripened into actual harm. This was a preemptive strike by the Bureau against a system it thought was insufficiently protecting consumer data, and a clear message that if you are subject to Bureau jurisdiction, it will not wait until a breach to protect consumers. Rather, the Bureau will be proactive in enforcement actions and supervisory actions where you have created the conditions for a breach.

Moreover, this position on protecting consumer data is consistent with recent Bureau actions against lead generators and their sharing of consumer personal information.[2] While those cases were not strictly data privacy matters, they reflected a similar concern as in the Dwolla case, with the Bureau's statements indicating that it wants to ensure that

[1] CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices, http://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/.

[2] CFPB Takes Action Against Lead Aggregators for Online Trafficking of Personal Information, http://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-lead-aggregators-for-online-trafficking-of-personal-information/.

consumer information is protected and does not fall into the wrong hands.

In addition, while this was a deception case, the consent order does contain hints that the Bureau believes there are certain minimal data security standards that are required – that there are "reasonable measures" which all companies need. This is reminiscent of the FTC's Wyndham action, where the FTC found a lack of certain minimum standards to be unfair under Section 5 of the FTC Act.[3] And while the Bureau has not set out a floor of minimally acceptable security practices, it has been suggested that regulated entities should be looking to regulatory pronouncements and guidance, consent orders, and industry best practices to tease out minimum standards and potentially develop plans that will allow them to defend against future allegations by the Bureau, other regulators, or private plaintiffs that even non-deceptive conduct is insufficiently protecting consumer data.

In the current environment, corporate decisions about data security must consider the reputational, regulatory, financial, and litigation risks that may result from inevitable breaches. These risks can be substantial and likely hinge on the reasonableness of a company's security protocols, both in the evaluation of existing protections and in the implementation of improvements. Companies need to make critical assessments concerning risks, controls, and gaps (for example, by using the FFIEC cybersecurity assessment tool). As the laws, regulations, and regulatory expectations concerning data security continue to develop, there will continue to be great interest in whether the most effective method for the various regulators and law enforcement agencies will be through the use of guidance and enforcement actions. Notwithstanding the uncertainty that remains, paying close attention to regulatory activity and guidance will provide valuable insight into areas of priority.

III. Conclusion

Data security is rapidly gaining more attention as a consumer protection issue. State and federal regulatory is certain to increase, in the form of guidance, supervisory findings, and enforcement actions. This is no longer just an "IT" problem, and the time is now to make it a compliance priority.

[3] FTC Files Complaint Against Wyndham Hotels For Failure to Protect Consumers' Personal Information, https://www.ftc.gov/news-events/press-releases/2012/06/ftc-files-complaint-against-wyndham-hotels-failure-protect; *see also FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

You're Invited! ABA Programming

Consumer Privacy and Data Security Developments

January 23, 2017, 12:00 – 1:00 PM ET

This hour-long session provides privacy law practitioners with timely and relevant updates on consumer privacy and data security activities covering regulation, legislation, and litigation in the United States and internationally.

Moderator:
- Mathew Sullivan

Speakers:
- Ilunga Kalala, Dana Beth Rosenfeld, Sherrie Kim Schiavetti, and Crystal N. Skelton

Click here for more information and to register.

Member Benefit: Access Past Committee Program Audio Recordings

The Section of Antitrust Law's Committee Programs are informal educational events on timely topics that typically last 60-90 minutes. As a benefit to Section members, these Committee Programs are available in an MP3 format at no charge. Section members can download the MP3 file to their computers and transfer the content to a portable MP3 player (such as an iPod or other digital audio player) or burn it to a DS.

To listen to or save a Committee Program, click here.

If you need assistance, contact Diana Odom at (213) 988-5702 or Diane.Odom@americanbar.org.

Self-Regulation of Interest-Based Advertising and Cross-Device Tracking

By Dana Rosenfeld and Devon Winkles

Dana Rosenfeld is a partner in Kelly Drye & Warren LLP's Washington, DC office and chair of the Privacy and Information Security practice. She was named 2017 D.C. Advertising "Lawyer of the Year" by Best Lawyers®. A former assistant director of the FTC's Bureau of Consumer Protection and attorney advisor to FTC Chairman Robert Pitofsky, Ms. Rosenfeld's practice focuses on all facets of privacy and data security, advertising, and consumer financial protection issues at the federal and state level. Her work includes recent matters for financial services institutions and their service providers, major retailers, direct marketers, consumer product manufacturers, and technology and telecommunications companies. Many of her matters focus in particular on emerging technologies, including mobile and "Big Data"-related services. She frequently represents clients before the FTC, the Consumer Financial Protection Bureau (CFPB), and state Attorneys General. These matters include law enforcement investigations and advocacy in connection with FTC and CFPB rulemaking proceedings, as well as industry initiatives seeking agency engagement on consumer protection regulatory issues, legislation, or enforcement policy.

Devon Winkles is an associate in Kelly Drye & Warren LLP's Washington, DC office. Ms. Winkles's experience includes advising clients on advertising claim substantiation, product labeling and packaging, and various other questions relating to advertising, marketing, endorsements, social media, promotions, product quality and safety, and collection and use of consumer information. She has worked with clients' legal, marketing, and research teams to develop advertising claims for new products and products under consideration, and to comply with new regulatory requirements. She regularly applies U.S. Food and Drug Administration (FDA), FTC, and National Advertising Division (NAD) standards and guidance to assess risks and opportunities for her clients.

Since the first beer ad aired during a football game, companies have been trying to reach their target audience—the folks with whom their message is most likely to resonate. This makes sense; companies are interested in converting their ad dollars to product sales as efficiently as possible. In recent years, the advertising industry has matured beyond the beer-and-football model, using technologies that allow companies to target consumers not only based on what TV shows they watch and what newspapers they read, but also based on past purchasing behavior, browsing history, precise location information, personal demographic information, expressed interests, and other data gathered over time. And in addition to reaching consumers through TV and print ads, advertisers place thumbnails and banner ads on third party websites and social media sites, serve in-app offers, and send targeted emails. In this way, the one-size-fits all marketing of the past can be replaced with customized messages. Browsing for a product online? You might see that product in an ad on a third party webpage a few minutes later. Marketers have a vast array of new tools at their disposal to reach their ideal audience and to reach that audience in a more effective way. Targeted marketing also can benefit consumers, providing them with information and offers that are most relevant to them. And because interest-based advertising is so effective, more online content can be supported by targeted ads and offered for free to consumers.

While traditional interest-based advertisers can use information about a user gathered on a single device and target that user on that device, increasingly companies are using technologies to track and target users across multiple devices. This "cross-device tracking" enhances traditional interest-based advertising by providing companies with consumer information across devices to better understand consumer behavior, and by allowing for targeted ads to be served across devices. In addition to the benefits of traditional targeted ads, cross-device tracking also allows for better "attribution": If a consumer is served an ad on a tablet but buys the product on a desktop, cross-device tracking can be used to recognize that link whereas single-device tracking cannot. Cross-device tracking can also be used to detect fraud; for instance, when a user logs in to a site from a new device, the consumer can be alerted to ensure the login is not fraudulent.

But as these tools have gained ubiquity, consumer privacy concerns have arisen. How are companies collecting and storing all of that consumer information? Are they collecting sensitive information, such as health data, financial information, or information about children? With whom are they sharing it? What risks are there to personal privacy? What options do consumers have for controlling use of their information in this way?

In this article, we will discuss the organizations working to balance the benefits of interest-based advertising with privacy concerns and creating frameworks for self-regulation.

I. The FTC's Self-Regulatory Principles

The FTC has authority to oversee privacy practices related to interest-based advertising (sometimes called "online behavioral advertising"), and in some cases has used this authority.[1] However, the FTC has encouraged the development of effective industry-led initiatives for regulating interest-based advertising. To that end, in December 2007, after receiving initial input from the public, FTC staff released a proposed set of principles for self-regulation and solicited additional public comments. In February 2009, the FTC staff issued a report titled "Self-Regulatory Principles for Online Behavioral Advertising," which responds to those comments and set forth revised principles.

Importantly, the Principles are not limited in scope to only classes of information that are traditionally understood as "personally identifiable information" or "PII." Rather, any data collected for online behavioral advertising that reasonably could be associated with a particular consumer or with a particular computer or device is within the scope of the Principles.

However, the Principles do contain two key carve-outs in that they do not apply to "first-party" and "contextual" advertising. "First-party" behavioral advertising occurs when a website collects consumer information to deliver targeted advertising at its own site and does not share any of that information with third parties. "Contextual" advertising involves targeting based on the webpage a consumer is viewing or a search query the consumer has made, and involves little or no data storage. The FTC determined that fewer privacy concerns may be associated with "first-party" and "contextual" advertising than with other behavioral advertising, and thus it concluded that it is not necessary to include such advertising within the scope of the Principles. Regardless of the scope of the Principles, companies must still comply with all applicable privacy laws.

The Self-Regulatory Principles are:

- **Transparency and Consumer Control:** Websites and platforms where information is collected for interest-based advertising should (1) disclose that data about consumers' activities online is being collected for use in providing interest-based advertising; (2) explain that consumers can choose whether to have their information collected for such purpose; and (3) provide consumers with a clear, easy-to-use, and accessible method for exercising this option.

- **Reasonable Security and Limited Data Retention for Consumer Data:** Companies that collect and store consumer data should provide reasonable security based on the sensitivity of the data, the nature of a company's business operations, the types of risks a company faces, and the reasonable protections available to a company, and companies should retain data only as long as is necessary to fulfill a legitimate business or law enforcement need.

- **Affirmative Express Consent for Material Changes to Existing Privacy Promises:** Before a company can use previously collected data in a manner materially different from promises the company made when it collected the data, it should obtain affirmative express consent from affected consumers.

[1] *See, e.g.*, *In the Matter of Epic Marketplace, Inc.*, FTC Matter No. 112 3182, Decision and Order (Mar. 13, 2013).

- **Affirmative Express Consent to (or Prohibition Against) Using Sensitive Data for Behavioral Advertising:** Companies should collect sensitive data (such as data about children, health, or finances) for behavioral advertising only after they obtain affirmative express consent from the consumer to receive such advertising.

II. The Self-Regulators

Based on the guidance from the FTC, several organizations have developed self-regulatory programs for interest-based advertising. The most comprehensive program is organized by the Digital Advertising Alliance (DAA), a consortium of advertising and marketing trade groups including the American Association of Advertising Agencies, the American Advertising Federation, the Association of National Advertisers, the Better Business Bureau, the Direct Marketing Association, the Interactive Advertising Bureau, and the Network Advertising Initiative. The DAA has issued its Self-Regulatory Principles and other guidance. It enforces these standards through cooperation with the Council of Better Business Bureaus' Interest-Based Advertising Accountability Programs, and has developed tools such as AdChoices to facilitate compliance. However, the DAA is not the only actor in this space. Most notably, the Network Advertising Initiative—a trade group for ad networks, platforms, optimization firms, and others—and the Direct Marketing Association—a trade group focused on data-driven marketing—each have their own standards and enforcement programs:

Program / Organization	Description	Applicability	Standards
Digital Advertising Alliance (DAA)	A consortium of the leading national advertising and marketing trade groups that together deliver self-regulatory solutions to online consumer issues	Principles extend to all companies involved in interest-based advertising—"first parties," "third parties," and "service providers"; certain programs are voluntary	• DAA Self-Regulatory Principles • Application of Self-Regulatory Principles to the Mobile Environment • Application of the DAA Principles of Transparency and Control to Data Used Across Devices • Self-Regulatory Principles for Multi-Site Data
AdChoices / AppChoices	Mechanism for satisfying DAA-enhanced notice requirements and Consumer Control Principle for desktop, mobile, and mobile apps	Voluntary participants	
Better Business Bureau's Interest-Based Advertising Accountability Program	Enforcement/accountability mechanism for the DAA Principles	Jurisdiction extends to all companies involved in interest-based advertising – "first parties," "third parties," and "service providers"—regardless of participation in DAA programs	

Program / Organization	Description	Applicability	Standards
Network Advertising Initiative (NAI)	Third-party digital advertising companies have established a set of self-regulatory principles that require members to provide notice and choice with respect to interest-based advertising and ad delivery and reporting activities	Member companies, including ad networks, exchanges, platforms, creative optimization firms, yield optimization firms, sharing utilities, and other technology providers	• Code of Conduct • Mobile Application Code • Guidance for NAI Members: Use of Non-Cookie Technologies for Interest-Based Advertising Consistent with the NAI Principles and Code of Conduct
Direct Marketing Association (DMA)	The world's largest trade association dedicated to advancing and protecting responsible data-driven marketing; develops and enforces Ethical Guidelines	All companies involved in direct marketing, regardless of membership	• DMA Guidelines for Ethical Business Practice

A. The Digital Advertising Alliance and the BBB Accountability Program

The DAA is a consortium of the leading national advertising and marketing trade groups, with the specific purpose of creating a self-regulatory system for interest-based advertising. In 2009, the DAA issued its Self-Regulatory Principles for Online Behavioral Advertising:

- **The Education Principle:** Calls for organizations to participate in efforts to educate individuals and businesses about online behavioral advertising.

- **The Transparency Principle:** Calls for clear and easily accessible disclosures, including enhanced notice, to consumers about data collection and use practices associated with online behavioral advertising.

- **The Consumer Control Principle:** Calls for providing consumers with an expanded ability to choose whether data is collected and used for online behavioral advertising purposes using a link on the webpage where the data is collected, and requires "service providers" to obtain the consent of users before engaging in online behavioral advertising, and take steps to de-identify the data used for such purposes.

- **The Data Security Principle:** Calls for organizations to provide appropriate security for and limited retention of data collected and used for online behavioral advertising purposes.

- **The Material Changes Principle:** Calls for obtaining consumer consent before a Material Change is made to an entity's data collection and use policies unless that change will result in less collection or use of data.

- **The Sensitive Data Principle:** Recognizes heightened protection for data collected from children and certain health and financial data when attributable to a specific individual.

- **The Accountability Principle:** Calls for development of programs to monitor and report instances of uncorrected noncompliance with the DAA Principles to appropriate government agencies.

The DAA Principles apply to all companies, not only those who have agreed to participate in the program.[2] The DAA Principles are enforced by the Council of Better Business Bureau's Internet-Based Advertising Accountability Program. The program, overseen by the organization that also oversees the National Advertising Division self-regulatory program, identifies potential cases of noncompliance with the DAA Principles. Often, the Accountability Program will ask the company to demonstrate its compliance. If further review is warranted, the Accountability Program will begin a formal review and ultimately release a public decision. If the company does not comply with the program's recommendation, the program can refer the matter to the appropriate federal agency.

The DAA Principles extend not only to single-device interest-based advertising but also to tracking across multiple devices, a topic the DAA covered in guidance released in November 2015. (It has also issued guidance on applying the DAA Principles to mobile devices, and has issued principles for the collection of multi-site data, extending beyond collection of data for interest-based advertising.) For example, in one case example involving cross-device tracking, the Accountability Program held that the use of device identification technologies that link multiple devices to a user or household should be clearly disclosed in company privacy policies. In addition, companies should make clear that opt-out preferences must be exercised on each device separately, as the current opt-out tools (such as those described below) are device- and browser-specific.

In addition to establishing this self-regulatory framework, the DAA has also developed the following *voluntary* tools that can facilitate companies' compliance with the DAA Principles:

- **AdChoices Icon:** Informs consumers that information may be used for targeted advertising, and clicking on the icon (which is usually found in the top corner of an online advertisement) will provide information about the companies behind the ad and an opportunity to opt out from receiving targeted ads from those participating companies.

- **YourAdChoices and aboutads.info/choices Page:** Allows consumers to opt out from the collection of web viewing data for interest-based advertising and other applicable uses, by some or all participating companies.

- **AppChoices App:** Allows consumers to opt out from mobile interest-based advertising with a particular participating company, or "Choose All Companies."

B. The Network Advertising Initiative

The NAI is a self-regulatory body governing advertising technology provided in the online advertising space. It was created by the online advertising industry in 2000 and has nearly 100 member companies, including ad networks, exchanges, platforms, creative optimization firms, yield optimization firms, sharing utilities, and other technology providers. The NAI Code of Conduct is a set of self-regulatory principles that require NAI member companies to provide notice and choice with respect to interest-based advertising and related ad delivery and reporting activities. The Code addresses the types of data that member companies can use for advertising purposes and imposes a host of substantive restrictions on member companies' collection, use, and transfer of data used for interest-based advertising. In many respects, the Code reflects the obligations set forth in the DAA Principles. One key difference between the DAA's

[2] Like the FTC's Self-Regulatory Principles, the DAA Self-Regulatory Principles do not extend to first-party collection of data through a site for the first party's own use.

self-regulatory system and the NAI's is that the Code applies only to NAI member companies.

The NAI enforces the Code through the new member onboarding process and through monitoring of existing members. If NAI staff finds during any of the compliance processes that a member has materially violated the Code, then NAI staff may refer the matter to the Board of Directors with a recommendation for sanctions. The member company may be given the opportunity to address the Board and respond to a staff finding of noncompliance. If the NAI Board of Directors determines that the member has committed a material violation, then the NAI may impose sanctions, including suspension or revocation of membership and may refer the matter to the FTC. Further, the NAI may publicly name a company or the violation in its annual compliance report.

In the 2015 update to the Code of Conduct, the NAI stated its intent to develop and issue guidance in regarding the application of the Code, including the application of the opt-out mechanism, to the collection of data across devices and the linking of multiple devices used or likely used by the same user or household. The NAI encouraged its members to consider the privacy principles set forth in the Code in adopting cross-device practices.

C. The Direct Marketing Association

The DMA is a trade association for organizations involved in data-driven marketing, including interest-based advertising. Unlike DAA and the NAI, the DMA's role expands beyond self-regulation into industry advocacy, facilitating networking, and other member resources.

As a DAA member organization, the DMA encourages its members to comply with the DAA Principles. In addition to the DAA Principles, the DMA's Guidelines for Ethical Business Practice are intended to provide generally accepted principles of conduct, covering a wide range of topics, including clarity of offers, decency, negative option marketing, price comparisons, marketing to children, and telephone marketing. Most relevant for our current purposes, Articles 31 through 37 of the Ethical Guidelines address the collection, use, and maintenance of marketing data, and Articles 55 through 58 address certain aspects of mobile marketing, such as mobile opt-out requests.

The DMA accepts consumer inquiries and other external reports of potential noncompliance. Companies found to be out of compliance with DMA's Ethical Guidelines can be reported to the DMA, regardless of whether they are DMA members. The DMA can refer such companies to the appropriate authorities, and DMA members that are out of compliance can be suspended from DMA membership.

III. Conclusion

Technology related to interest-based advertising, cross-device tracking, and control mechanisms is quickly evolving. But the general principles outlined by the FTC and self-regulatory organizations are universally applicable to these forms of targeted marketing. Companies should look to the self-regulatory organizations, including the DAA, NAI, and DMA, and related enforcement activity for guidance on applying these principles in their businesses.

Like what you see in this edition?

Want to get more involved?

Please contact Ashley Rogers at arogers@gibsondunn.com.

FTC Enforcement Actions Address False "All Natural" Claims

By Katrina Robson, Hannah Chanoine, and Tristan Bufete

This article is a summary for general information and discussion only and may be considered an advertisement for certain purposes. It is not a full analysis of the matters presented, may not be relied upon as legal advice, and does not purport to represent the views of our clients or O'Melveny & Myers LLP.

Katrina Robson, an O'Melveny partner licensed to practice law in California and the District of Columbia, Hannah Chanoine, an O'Melveny counsel licensed to practice law in Massachusetts and New York, and Tristan Bufete, an O'Melveny associate licensed to practice law in California, contributed to the content of this article. The views expressed are the views of the authors except as otherwise noted.

Litigation over the term "natural" is not new, partly because for many product categories, there is no regulatory definition for the term. While the Food and Drug Administration considers whether it should define "natural" in food labels,[1] the Federal Trade Commission (FTC) has recently weighed in on how its use might be deceptive for the advertising of personal care products (PCP). Specifically, on July 13, 2016, the FTC announced that it had approved final consent orders against four companies that allegedly misrepresented their PCPs as "all natural" or "100 percent natural," despite the fact that the products contained synthetic ingredients.

I. The "Natural" Personal Care Products Industry

PCPs generally refer to the variety of items commonly found in the health and beauty sections of drug and department stores.[2] The "natural" PCP market is worth approximately $5 billion per year, and according to one estimate, is projected to increase at a 6% annual clip for the next three years.[3] It comes as no surprise, then, that as the market for natural products has increased, so has litigation regarding natural claims on PCPs.

PCPs, of course, are not the only products that are the target of consumer class action litigation over the use of "natural," "all natural," or similar descriptions. In the last five years hundreds of class action claims have been filed over the use of these terms across a range of industries, including most notably the food and beverage business. Still, PCPs are routine targets. In just the past few months, for example, the manufacturers of lip balm, hand soap, shampoo, and bubble bath have been sued on theories that the term "natural" is deceptive.[4] These suits are typically brought under state consumer protection statutes (as well as under state common laws). Until now, however, the FTC has not weighed in on the use of these terms in advertising.

II. The Allegations and Final Settlements

In its first enforcement actions under Section 5(a) and/or Section 12 of the FTC Act against companies that market PCPs with misleading "natural" claims, the FTC filed administrative complaints against the following[5]:

---

1 *See FDA Requests Comments on Use of the Term "Natural" on Food Labeling*, U.S. FOOD & DRUG ADMIN. (last updated Dec. 24, 2015), *available at* http://www.fda.gov/Food/NewsEvents/ConstituentUpdates/ucm471919.htm.

2 The term "personal care product" is not defined by law. *Are all "personal care products" regulated as cosmetics?*, U.S. FOOD & DRUG ADMIN. (last updated May 22, 2016), *available at* http://www.fda.gov/ForIndustry/FDABasicsforIndustry/ucm238796.htm.

3 Serena Ng, *FTC Charges Five "Natural" Products Firms Over Claims*, WALL ST. J. (Apr. 13, 2016, 2:57 PM), *available at* http://www.wsj.com/articles/ftc-charges-five-natural-products-firms-over-claims-1460500050.

4 *See, e.g.*, *Tyman v. Pfizer, Inc.*, No. 1:16-cv-06941-LTS (S.D.N.Y.); *Hiddlestone v. The Honest Co.*, No. 2:16-cv-07054-JAK-AGR (C.D. Cal.); *Buonasera v. The Honest Co.*., No. 1:16-cv-01125-VM (S.D.N.Y.)

5 The FTC also filed an administrative complaint against a fifth company, California Naturel Inc., alleging that the company's "all natural" representation on its sunscreen product was false or misleading because it contained the synthetic ingredient Dimethicone. The FTC's July 1, 2016 status report notified the

TransIndia Products Inc., doing business as ShiKai: The FTC alleged that TransIndia Products' "all natural" representations on its lotion and shower gel were false or misleading because the products contained some or all of the following synthetic ingredients: Dimethicone, Ethylhexyl Glycerin, and Phenoxyethanol.

Erickson Marketing Group Inc., doing business as Rocky Mountain Sunscreen: The FTC alleged that Erickson Marketing Group's "all natural" representations on its sunscreens were false or misleading because the products contained the following synthetic ingredients: Dimethicone, Polyethylene, Butyloctyl Salicylate, and Neopentyl Glycol Diethylhexanoate.

ABS Consumer Products LLC doing business as Eden Bodyworks: The FTC alleged that ABS Consumer Products' "all natural" representations on its hair care products were false or misleading because the products contained a range of synthetic ingredients, including: Polyquaternium7, Phenoxyethanol, and Caprylyl Glycol.

Beyond Coastal LLC: The FTC alleged that Beyond Coastal's claim that its sunscreen was "100 percent natural" was false or misleading because it contained the synthetic ingredients Dimethicone and Caprylyl Glycol.

In the final consent orders, each of these four companies agreed not to misrepresent the following when advertising, promoting, or selling its products:

- Whether a product is all natural or 100 percent natural,
- The extent to which a product contains any natural or synthetic ingredient or component,
- The ingredients or composition of the product, and
- The environmental or health benefits of the product.

Moreover, each of the companies agreed to have and rely on "competent and reliable evidence" to substantiate the claims that it makes about a product's ingredients, environmental benefits, or health benefits, which is defined as "tests, analyses, research, studies or other evidence based on the expertise of professionals in the relevant area, that have been conducted and evaluated in an objective manner by qualified persons, using procedures generally accepted in the profession to yield accurate and reliable results." If the professionals in the relevant area would require "reliable scientific evidence," the companies are no longer allowed to rely on "other evidence" but must instead offer evidence from one of the other four categories: tests, analyses, research or studies.

Takeaway #1: Companies Should Exercise Caution When Using the Claim "All-Natural" or "100% Natural" on Products with Synthetic Ingredients or Chemicals.

As the FTC noted in its announcement of the tentative settlements, marketers should understand that "'all natural' or '100% natural' mean just that."[6] If a company advertises a product containing synthetic ingredients or chemicals but markets the product as "all natural" or "100% natural," "now is the natural time for a compliance check."[7]

The FTC also cautioned that if a reasonable consumer would interpret an advertisement touting a product as "natural" to mean that the product is "all

administrative law judge that a tentative settlement had been reached. However, the FTC has been unable to finalize the agreement and withdraw the matter from adjudication. *In re Cal. Naturel, Inc.*, F.T.C. Docket No. 9370, Complaint Counsel's Second Status Report (July 1, 2016).

6 Lesley Fair, *Are your "all natural" claims all accurate?*, FED. TRADE COMM'N BUS. BLOG (Apr. 12, 2016, 1:13 PM), https://www.ftc.gov/news-events/blogs/business-blog/2016/04/are-your-all-natural-claims-all-accurate.

7 *Id.*

natural," the claim *would* violate the final orders.[8] The FTC also noted that the advertisement would be evaluated "as a whole,"[9] suggesting that if a company advertised a product containing synthetic ingredients as "natural" and paired that term with other language or images implying that the product was 100 percent natural, it would violate the terms of the order.

Takeaway #2: While Using "Natural" in Products with Synthetic Ingredients Continues to Pose Risk, the FTC Confirmed That "Natural" is* Not *the Same as "All-Natural."

The FTC sought public comments before finalizing the consent orders. Notably, the FTC declined to adopt one commentator's suggestion that products should not be represented as "natural" if they contain any amount of synthetic ingredients, implying (said the FTC) that the consent agreements should prohibit the claim "natural" unless the product is "all natural" (i.e., contains no synthetic ingredients).[10] The FTC explained that it lacked evidence that consumers interpret the term "natural" to mean "all natural" or no synthetic ingredients. Accordingly, companies still lack a regulatory definition for the term "natural" for the time being, meaning that companies should navigate its use with care, especially where the advertised product contains synthetic ingredients.

In these actions, the FTC focused primarily on the modifiers "100 percent" and "all" in "100 percent natural" and "all natural" rather than the word "natural" alone. However, these recent enforcement actions signal that the use of such claims in advertising is not immune from scrutiny by the FTC.

8 Letter from Donald S. Clark, Secretary of the Commission, to Ms. Mia Hardwick (July 6, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/1607ltrstocomments.pdf.

9 *Id.*

10 *E.g.*, *id.*