Federal Trade Commission

Consumer Protection 2015: Back to Basics for the New Media

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

Kelley Drye & Warren LLP – Advertising and Privacy Law Summit
June 11, 2015

I'm delighted to be here to kick off this interesting event. I'd like to use my time this morning to talk about the FTC's latest work in advertising and privacy. That's much broader than the Internet of Things, the unifying theme for this event. But the Internet of Things is indeed a fitting backdrop since it encapsulates many of the broader consumer protection challenges we face today.

For starters, data is collected from and about consumers wherever they go – through their smartphones, wearables and fitness devices; in their smart homes and smart cars; as they shop in stores and online; as they check and update their many social networks; as they walk down the street; everywhere.

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

Advertising, too, is coming at consumers from every angle, through their many smart devices, in every conceivable format. Fantastical products make fantastical claims. Companies send you ads about cures for that cold you just caught yesterday. Those shoes you viewed online five minutes ago follow you everywhere. Everyone's a salesman – your friends on Facebook, and even that six-year old unwrapping gifts on his own YouTube channel, EvanTube. And providing effective disclosures amidst this cacophony is a real challenge.

The FTC's current priorities in advertising and privacy reflect these challenges. Our goal is to make clear that the fundamental principles of consumer protection still apply to today's and tomorrow's marketplace. Sure, they need to be adapted and updated. But the basic rules still apply.

Tell the truth. Disclose any facts necessary to prevent a claim from being misleading. 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 eternal. They apply to the Internet of Things, Big Data, Native Advertising, the Sharing Economy, mobile apps, blogs and sponsored content, new payment platforms, and most of what we see in the consumer marketplace today.

I. Advertising

Let me turn to some of our recent activities along these lines. I'll talk first about advertising and, in particular, false or unsubstantiated health claims, deceptive endorsements, and buried disclosures.

Deceptive Health Claims

Deceptive health claims are a longstanding FTC concern. Today, with the proliferation of health apps and consumers' strong focus on health, they remain the FTC's top advertising priority.

We brought many cases over the past year challenging a range of health claims. For example, the FTC recently charged two app developers with deceptively claiming that their mobile apps – Mole Detective and MelApp – could detect symptoms of melanoma, even in the early stages. Each company claimed that its app used a mathematical algorithm to measure the characteristics of moles for melanoma. In fact, we alleged, the companies lacked the evidence to show that their apps could detect melanoma, early or at all.

We also continue to be concerned about false and unsubstantiated weight loss claims – you know, claims that pills, potions, and powders will allow you to drop weight miraculously without any diet or exercise. This year, our cases in this area include three that involved the purported slimming effects of pure green coffee bean extract, which had been featured on *The Dr. Oz Show*.

In one case (*NPB Advertising*), we alleged that the defendants set up fake news sites that made false claims about the effectiveness of the supplement and channeled people to another site where they could buy it. In another, we charged, defendant Lindsey Duncan made TV appearances touting pure green coffee bean extract, purporting to be an independent expert, when he was actually selling the supplement – deceptively – through websites set up just beforehand. In the third, we took action against Applied

Food Sciences for allegedly disseminating a flawed, indeed doctored, study purporting to prove the efficacy of the supplement.

We're also seeing many health claims targeted at particular age groups, especially older adults and young children. According to the Pew Research Center, nearly half of adults in their 40s and 50s have both a parent age 65 or older, and are either raising a young child or financially supporting a grown child.[2] If you fall within this group, you may be seeing ads for products offering cognitive and memory benefits, as well as other age-related treatments.

Many of them aren't true, of course. Last month, we filed a case against Lunada Biomedical alleging false and unsubstantiated claims about Amberen, a supplement for women over 40. The company claimed that the supplement could cause significant loss of weight and belly fat, and "restore hormonal balance naturally the weight can just fall right off."

Then, there are the cognitive games for young children. In January, 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. It would be wonderful if a game could do that, but we alleged, again, that the claims were false and unsubstantiated.

And in October, we filed suit against Gerber, alleging unsubstantiated claims for its Good Start Gentle infant formula. Gerber advertised that the formula would reduce

[2] Pew Research Center, *The Sandwich Generation: Burdens on Middle-Aged Americans on the Rise*, May 15, 2013, *available at* http://www.pewresearch.org/daily-number/the-sandwich-generation-burdens-on-middle-aged-americans-on-the-rise/.

the risk of allergies, but we alleged that it didn't have sound scientific evidence to back that up. The case is pending in federal court.

Deceptive Endorsements

The second advertising area that I want to highlight is deceptive endorsements. With blogs and bloggers everywhere, and the explosive growth of social networks and new media, anyone can endorse a product and gain a wide audience doing it. The rules are pretty basic, even with all the new scenarios they apply to. To avoid deception, endorsements must be truthful and not misleading. If there's a connection between an endorser and the marketer of the product that would affect how people evaluate the endorsement, it must be disclosed clearly and conspicuously. And if the advertiser doesn't have proof that an endorser's experience represents what consumers will typically achieve, the advertiser must disclose the results that *would* be typical.

We've challenged deceptive endorsements in many of our health and weight loss cases, including several that I just mentioned. But given the ubiquity of reviews, blogs, and infomercials, we're seeing deceptive endorsements just about everywhere. In November, we took action against Sony for alleged deception in advertising the features of one of its gaming consoles. In a related case, we alleged that its ad agency, Deutsch, was complicit in the deception, and that one of its managers had asked its employees to post positive tweets about the console as part of its ad campaign. According to our complaint, the resulting tweets were deceptive because they did not reflect the views of actual consumers, and Deutsch failed to disclose the employees' connection to Deutsch and thus Sony.

In a similar vein, we took action against shipment broker AmeriFreight in February for failing to disclose that it provided discounts and awards to customers who posted reviews of its service.

Finally, to provide guidance in this important area, we recently updated the FAQs for our Endorsement Guides.[3] The revised FAQs take a deeper dive into forms of promotion that were relatively new when we did our last update – for example, Twitter, affiliate marketing, "like" buttons, employee endorsements, solicited endorsements, and uploaded videos, to name just a few.

Clear and Conspicuous Disclosures

Finally, I want to address a significant issue that runs through all of our work – disclosures. By disclosures, I mean information needed to prevent an ad from being deceptive. The law is pretty basic here too: Disclosures must be clear and conspicuous. To accomplish this, advertisers should use direct and unambiguous language and make the disclosure stand out. If a disclosure is hard to find, tough to understand, buried in unrelated details, or obscured by other elements in the ad, it's not clear and conspicuous. This is true not just in print, but online and on mobile. We have an excellent guidance piece on this – *Dot Com Disclosures*, which we recently updated to provide specific guidance for making disclosures on mobile devices, Twitter, and other new media.[4]

Many of our cases involve problems with omitted or buried disclosures. So last year, we launched a project called *Operation Full Disclosure* to remind companies of the

[3] *The FTC's 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.

[4] *.com Disclosures: How to Make Effective Disclosures in Digital Advertising* (Mar. 2013), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/com-disclosures-how-make-effective-disclosures-digital.

importance of clear and conspicuous disclosures. We contacted over 60 companies, including 20 of the biggest advertisers in the country, to alert them to problems with disclosures in their TV and magazine ads. The response to our outreach has been very positive but you can expect more work in this area.

On the Horizon

That's a snapshot of our advertising work this year, and I haven't even talked about our extensive work on green claims and auto ads, or our big case against DIRECTV. For the upcoming year, we'll continue to focus on health claims of all sorts, especially cognitive claims, as well as endorsements and disclosures. In the fall, we'll host a workshop on over-the-counter homeopathic products to examine how these products are being marketed and advertised. And we'll issue guidance on Native Advertising by the end of the year.

II. Privacy

Now I'll move to our privacy program. Earlier, I talked about the ubiquity of data collection. But it's also invisible in many ways. Most of the companies that collect consumers' data online and through their mobile devices are behind the scenes and never interact with consumers. And as we move into the era of the Internet of Things, data collection will become even more invisible.

Our privacy program focuses on three related areas designed to protect consumers in this environment – Big Data, Sensitive Data, and New Technologies.

Big Data

First is Big Data, by which I mean the vast collection of detailed data about consumers for use in making predictions about their behavior or likely outcomes.

Big Data can, of course, drive valuable innovation across many fields – medicine, education, transportation, and manufacturing. But it also raises privacy concerns for consumers – massive collection and storage of personal information; the risk that detailed profiles will fall into the wrong hands, enabling identity theft and other harms; the release of sensitive information consumers regard as private; and the potential use of this data by employers, insurers, creditors, and others to make important decisions about consumers.

Our central message is that, even in the face of rapidly changing business models and technologies, companies still need to follow the basic privacy principles. Don't collect or retain more data than you reasonably need. If you must collect it, consider de-identifying it to minimize any harm if it falls into the wrong hands. Tell consumers how you plan to use and share their data. Give consumers meaningful choices about their privacy. And protect consumer data from unauthorized access. As new business models and technologies develop, these principles remain relevant and important, although they do need to be adjusted and adapted.

We've emphasized these principles through both policy initiatives and enforcement. In January, we issued a staff report setting forth a number of recommended best practices for the Internet of Things.[5] One issue we addressed was the question we

[5] 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.

hear again and again about whether notice and choice have continuing relevance, 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.

In addition, last year, we hosted a workshop entitled *Big Data: A Tool for Inclusion or Exclusion?*[6] The workshop explored how the categorization of consumers may be both creating and limiting opportunities for consumers, with a focus on low income and underserved consumers. We plan to issue a report on this topic in the coming months. One of our main messages is – there are laws on the books that address many of these concerns and companies must comply with them.

For the past few years, we've also focused a lot of attention on the unique privacy challenged presented by the data broker industry. Last year, we issued a report on these entities, showing the enormous number of data points they collect on each consumer, the profiles and categories they use to characterize individuals, their many sources of data, and the clients they sell to – which *do* include employers, insurers, and creditors.[7] We also brought a number of cases against data brokers selling information for purposes covered by the Fair Credit Reporting Act without complying with that important law.

---

[6] *See generally* https://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion.

[7] FTC Report, *Data Brokers: A Call For Transparency and Accountability* (May 2014), *available at* https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014.

We remain very concerned about the invisibility of these practices to consumers. And it's not just about privacy. Increasingly, we are seeing a link between data brokers and fraud. In fact, we often discover in our fraud cases that the scammers used highly sensitive data bought from another company – including Social Security and bank account numbers – to trick or steal from consumers. This data goes well beyond the usual lead lists we've been seeing for years.

For example, in December, we brought action against data broker LeapLab. Our case alleged that LeapLab bought the payday loan applications of financially strapped consumers – which included names, addresses, phone numbers, employers, SSNs, and bank account numbers – and then sold this sensitive data to marketers whom it knew had no legitimate need for it. These marketers included phony internet merchants that used the information to withdraw millions of dollars from consumers' accounts without their authorization. We charged that LeapLab's sale of this data to scam artists and others it had reason to believe had no legitimate need for it was unfair under the FTC Act. This case is currently in litigation.

We also know that so-called phantom debt collectors – fraudsters that call consumers demanding payment of debts consumers don't owe – buy their sensitive leads from other companies. Finding and suing the people who sell this data is very difficult, but we have investigations underway similar to the *LeapLab* case.

We're also seeing careless handling of sensitive data by data brokers that puts that information at serious risk. For example, in December, we brought action against debt brokers Bayview and Cornerstone, alleging that they posted the sensitive data of more

than 70,000 consumers online – including bank account and credit card numbers, birth dates, contact information, and information about their debts – on a public website as part of their efforts to sell debt portfolios. The court in that case ordered that the data be taken down immediately and that consumers be notified.

Sensitive data

A second area of focus in privacy is safeguarding sensitive information – that is, kids', health, financial, and precise geolocation data. This has long been a priority for the Commission. But in today's marketplace, the stakes are even higher as sensitive data is captured all day long and then used and shared in ways consumers would never expect.

Health data is a chief concern because much of it falls outside of HIPAA, the law that everyone seems to *think* protects all health information. In fact, the protections of HIPAA are limited to medical providers like hospitals and insurance companies. HIPAA doesn't cover most health apps and consumer generated health data – but the FTC Act does.

In December, we charged Payments MD, a health billing company, with deceiving thousands of consumers who signed up for its online billing portal into also consenting to the collection of their detailed medical information from third parties. According to our complaint, defendants used a deceptive registration process to trick consumers into clicking boxes authorizing them to seek the records from pharmacies, medical labs, and insurance companies.

Then there are websites that harvest sensitive data, post it online, and seek payment to take it down. We took action against two of those this year. In one, the

defendant Craig Brittain solicited sexually explicit photos from women's ex-boyfriends and others – in many cases through deception – to post on his website, isanybodydown.com. He then used another site to pose as an attorney and charge $250 for removing the information. The Commission also issued a unanimous summary decision finding law violations by Jerk.com. That case involved photos of kids and teens being labeled a "jerk," supposedly by their peers.

Data security is also a huge part of our work to protection sensitive information. Over the past 15 years, we've brought over 50 enforcement actions against companies that failed to implement reasonable security protections – including companies such as Microsoft, TJX, Lifelock, and CVS. Our 50th case, announced last August, was against GMR Transcription Service, a company whose poor security practices, we alleged, exposed the medical information of thousands of consumers on the Internet. This year, we are taking our message on the road, gearing up for a campaign called *Start with Security*, in which we will host events around on the country on security topics and best practices. We also will continue to put out business guidance, including a new piece soon on lessons learned from FTC cases. The Commission, of course, also unanimously supports new federal legislation to enhance our authority in this area.

Finally, the FTC has a special interest in protecting the privacy of kids. To date, we've brought 25 cases in this area, including two COPPA cases last fall against the mobile app for Yelp and the gaming app *TinyCo*. Each company paid substantial civil penalties.

Mobile and Tech

A third area of focus for our privacy program is mobile technologies and, indeed, tech more broadly. In the past few years, this area has become one of the main priorities at the FTC – in privacy and more generally. For example, we've brought cases against Apple, Amazon, and Google related to kids' in-app purchases; against T-Mobile and AT&T for mobile cramming; and against AT&T and TracFone for making allegedly false claims that they provided "unlimited data" to their broadband customers. These cases are all about applying basic consumer protection rules to the growing mobile platform.

As to our privacy work around mobile and tech, I've already talked about *Yelp* and *TinyCo*, our COPPA cases involving two popular apps. And our IoT report, which I also discussed, is all about applying basic privacy principles to mobile and other new contexts. Over the past year, we also brought several actions involving mobile security, including our cases against the Fandango movie app and the financial app Credit Karma. In both cases, we alleged, the companies put consumers' sensitive information at risk by, among other things, disabling a critical default process known as SSL certificate validation that would have verified that the apps' communications were secure.

Part of our focus in tech is internal to the FTC – to make sure we have the personnel and resources to meet the consumer protection challenges of the expanding tech world. A few years ago, we created the Mobile Technology Unit to help bring consumer protection into the mobile era. The MTU assisted BCP staff with law enforcement investigations and policy reports. It also developed surveys on kids' apps, mobile shopping apps, and health apps. Recently, we announced that we would broaden

the MTU's mission so it focuses not just on mobile, but on tech more broadly. We renamed it the Office of Technology Research and Investigation (OTech), and are in the process of adding a couple more researchers and technologists. We expect the office to play an important role in the agency's work on privacy, data security, connected cars, smart homes, emerging payment methods, big data, and the Internet of Things. Stay tuned.

On the horizon

We have a lot of upcoming work in the privacy area but I'll highlight a few beyond the items I already mentioned. Health privacy will continue to be a focus. You'll see more cases related to the Internet of Things, as well as the sale of sensitive data to scammers. In the fall, we'll host our workshop on cross-device tracking to examine the various ways that companies now track consumers across multiple devices, and not just within one device. And of course, we'll be focusing generally on all of the areas I mentioned – Big Data, Sensitive Data, and Mobile and Tech.

III. Conclusion

So that's our list – it gives you a snapshot of our activities over the past year and upcoming priorities, perhaps more information than you want. I am happy to take questions – thank you for having me here today.