Federal Trade Commission

FTC Year in Review: Advertising and Privacy in the Age of Influencers, Smartcars, and Fitbits

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

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

I'm pleased to be here for what has become an annual update on the FTC's work and priorities in advertising and privacy. Last year, I focused on the challenges that new technologies pose for consumer protection, and how the basic rules of the road continue to apply to the marketplace. One year later, the explosive growth of new technology and media still drives much of what we're doing at the FTC. We're seeing more and more data collected from and about consumers, such as through health apps, smart cars, and other Internet of Things devices. Advertising is coming at consumers from all of these devices, in every conceivable format. And providing consumers with information and choices amidst this cacophony is as challenging as ever.

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

To address these issues, the FTC is bringing high visibility enforcement actions, issuing guidance to consumers and businesses, and bulking up our technological know-how at the agency. I'd like to highlight some of these efforts today.

I. Advertising

I'll start with advertising. Last year, I talked about three areas of focus for the coming year – health claims, endorsements, and native advertising. We've been busy in all three areas.

Deceptive Health Claims

The first area – deceptive health claims – has long been a priority, but the changing marketplace has created new ways to reach and deceive consumers.

For example, we're seeing more and more mobile apps marketed as medical devices. You may recall our earlier actions against apps that promised to cure consumers' acne, and apps that claimed to diagnose cancerous moles.[2] Last fall, we brought a similar action against vision improvement app Ultimeyes.[3] Ultimeyes claimed to have scientific proof that doing visual exercises on the app would "turn back the clock" on consumers' vision and reduce the need for glasses and contacts. In fact, we charged it had no such proof.

And speaking of turning back the clock, we're seeing many health claims targeted at older consumers – in a clear effort to tap into the anxieties (and wallets) of aging baby

[2] *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.

[3] *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.

boomers. In January, we settled charges that the Lumosity "brain training" program made unfounded claims that its games could help users perform better at work and in school, and could stave off memory loss, dementia, and even Alzheimer's disease.[4] As part of the settlement, Lumosity agreed to pay $2 million in redress and to provide subscribers with an easy way to cancel their annual subscriptions.

One interesting case this year involved athletic apparel company Tommie Copper.[5] We charged the company with making false or unsubstantiated claims that its copper-infused compression clothing would relieve severe and chronic pain and inflammation caused by arthritis and other diseases. The company paid $1.35 million to settle the case.

Another case – this one quite disturbing – involved Sunrise Nutraceuticals, the marketer of an addiction cure.[6] We charged this company with making false or unsubstantiated claims that its supplement Elimondrol could treat and even cure people who are addicted to opiates, including prescription pain medications and illegal drugs such as heroin. This case is pending in federal district court.

Deceptive Endorsements

Deceptive endorsements also continue to be a priority, especially given the rapid growth of newer forms of promotion, such as Twitter, "like" buttons, videos, and employee endorsements. We recently updated our Endorsement Guides to address these

[4] *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.
[5] *FTC v. 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.
[6] *FTC 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.

newer forms of promotion.[7] The key principle is pretty simple: consumers have a right to know when a supposedly objective opinion is actually a marketing pitch.

Unfortunately, many companies, including mainstream ones, still haven't learned this lesson. Recently, we charged Machinima, an entertainment network that worked for Microsoft's ad agency, with paying a large group of "influencers" to post videos online touting XboxOne.[8] The videos appeared to be the objective views of the influencers, and did not disclose they were actually paid endorsements. This is just one of many deceptive endorsement cases we've brought recently. You also may remember *Sony*, *Lindsey Duncan*, *Lunada*, *NourishLife*, *Legacy Learning*, and *ADT* – it's a long list.[9]

And, in another significant case 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 product from getting out.[10] The company had hidden a gag clause in the fine print of its terms and conditions, which we alleged to be unfair.

---

[7] *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.

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

[9] *Sony Computer Entertainment America LLC*, No. C-4514 (Mar. 24, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3252/sony-computer-entertainment-america-llc-matter; *FTC v. Genesis Today, Inc.*, No. 1:15-cv-00062 (W.D. Tex. filed Jan. 26, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3283/genesis-today-pure-health-lindsey-duncan; *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; *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; *Legacy Learning Systems, Inc.*, No. C-4323 (June 10, 2011), *available at* https://www.ftc.gov/enforcement/cases-proceedings/102-3055/legacy-learning-systems-inc-et-al-matter; *ADT LLC*, No. C-4460 (June 18, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3121/adt-llc-matter.

[10] *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.

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 about this practice.[11] It affirms that ads and marketing that promote the benefits and attributes of goods and services should be identifiable as advertising to consumers.

We also just brought our first native advertising case against retailer Lord & Taylor.[12] We alleged that the company deceived consumers by paying for native ads, including a seemingly objective article in an online fashion publication, without disclosing they were actually paid promotions for a 2015 clothing launch. We also challenged the company's endorsement practices, charging that it paid 50 online fashion "influencers" to post Instagram pictures of themselves wearing a dress from the new collection without disclosing that it had paid the influencers to do so.

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

II. Privacy

Now I'll move to our privacy program. In recent years, data collection and use, personalization and predictions, and round-the-clock tracking have just exploded.

---

[11] *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; *see also Native Advertising: A Guide for Businesses* (Dec. 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/native-advertising-guide-businesses.

[12] *Lord & Taylor, LLC*, No. C-4576 (May 23, 2016) , *available at* https://www.ftc.gov/enforcement/cases-proceedings/152-3181/lord-taylor-llc-matter.

Whether it's through a mobile device, Fitbit, smart car, social network, or thermostat, everyone is being tracked and profiled.

A critical goal of our privacy program is to keep pace with these developments, and we're fortunate to have the FTC Act to help us. The FTC Act is specifically designed to be flexible and to accommodate a changing marketplace. And over the years, we've used it to target a wide range of privacy practices, including deceptive claims about how data is collected and used; failure to protect sensitive data from unauthorized access; invasive spam and spyware; the sale of sensitive data to scam artists; and even extortion websites that post private data and demand money to remove it.

This morning, I'd like to talk about four areas of concern – health privacy, the Internet of Things, Big Data, and data security.

Health Privacy

I'll begin with health privacy. It seems like every day a company announces a new health-related app, device, or service. There are devices that allow consumers to track their diet and exercise; apps that track glucose levels; websites where patients with the same condition share information; and personal health records where consumers can store and manage their health information.

Much of this activity now takes place outside of hospitals and doctors' offices, so it's not covered by HIPAA. That's where the FTC Act comes in. It covers a lot of the

health data HIPAA covers and a lot it doesn't. It's a very important tool because health data is sensitive and personal, and consumers generally expect it to be private.[13]

We're doing what we can to stop illegal practices that compromise health information. For example, just this morning, we announced a settlement with Practice Fusion, a company that provides management services to physicians.[14] We alleged that the company deceived hundreds of thousands of consumers by soliciting reviews about their doctors without disclosing that the reviews would be posted publicly on the internet. As detailed in our complaint, many of the posted reviews included consumers' full names, medications, health conditions, and treatments received.

We also took recent action against Henry Schein Practice Solutions, a provider of office management software for dental practices. We alleged that Schein misrepresented that its software provided industry-standard, HIPAA-compliant encryption for sensitive patient information when it used a much weaker data-masking standard.[15] Our order prohibits the claims and requires Schein to notify its customers and pay $250,000 to redress its customers.

Because many of the entities collecting health data in today's marketplace are health apps and other small companies, we're also placing a lot of emphasis on business education. This year, we worked with HHS and the FDA to develop an interactive tool

---

[13] Erin McCann, *mHealth, Privacy Top Consumers' List of 2015 Health Industry Issues*, Healthcare IT News, Dec. 4, 2014, *available at* http://www.healthcareitnews.com/news/mhealth-privacy-top-consumers-list-2015-healthcare-issues (describing a study done by PricewaterhouseCoopers' Health Research Institute finding, among other things, that the majority (65%) of consumers consider data security more important than convenient access to medical imaging results, physicians' notes, diagnoses, and prescriptions).

[14] *Practice Fusion, Inc.*, Matter No. 1423039 (June 8, 2016) (proposed consent), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3039/practice-fusion-inc-matter.

[15] *Henry Schein Practice Solutions, Inc.*, No. C-4575 (May 23, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3161/henry-schein-practice-solutions-inc-matter.

showing app developers which laws apply to them, whether it be HIPAA, the Food, Drug, and Cosmetic Act, the FTC Act, or the FTC's Health Breach Notification Rule.[16] In conjunction with this project, the FTC also released guidance to help mobile health app developers build privacy and security into their apps.[17]

Internet of Things

The Internet of Things is also an expanding part of our work. It *has* arrived, and it comes in the form of fitness devices, wearables, smart cars, and connected smoke detectors, light bulbs, and refrigerators. These products are innovative and exciting. 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 some 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.[18] Our recent case against computer hardware company ASUS illustrates the problems created by poor device security.[19] Our complaint charged that critical security flaws in ASUS' routers put the home networks of hundreds of thousands of consumers at risk. You may also recall our case against TRENDnet, which compromised the security of home security monitoring cameras.[20]

---

[16] *See* Mobile Health Apps Interactive Tool (Apr. 2016), *at* https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool.
[17] *See Mobile Health App Developers: FTC Best Practices* (Apr. 2016), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices.
[18] *See, e.g.*, Charlie Miller & Chris Valasek, *Remote Exploitation of an Unaltered Passenger Vehicle* (2015), *available at* http://illmatics.com/Remote%20Car%20Hacking.pdf.
[19] *ASUSTeK Computer Inc.*, Matter No. 1423156 (Feb. 23, 2016) (proposed consent), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3156/asustek-computer-inc-matter.
[20] TRENDnet, Inc., No. C-4426 (Jan. 16, 2014), *available at* http://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter.

Last year, the FTC issued a report addressing how fundamental privacy principles can be adapted to Internet of Things devices and recommending best practices for companies to follow.[21] The FTC also just submitted a comment to NTIA on this topic.[22] You can expect the Internet of Things to become an even greater priority as it expands across the marketplace.

Big Data

Another area of concern is Big Data, by which I mean the vast collection of data about consumers to make predictions about populations or groups of consumers. Here again, there are many potential benefits, including to public health and safety. But the increase in data collection and storage also increases the risk of data breach, identity theft, and the likelihood that data will be used in ways consumers don't expect or want.

We recently issued a report entitled *Big Data: A Tool for Inclusion or Exclusion?* addressing how the categorization of consumers may be both creating and limiting opportunities for them, with a focus on low income and underserved consumers.[23] 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, and that must be complied with.

---

[21] 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.

[22] *Comment of the Staff of the Bureau of Consumer Protection and the Office of Policy Planning Before the NTIA: The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things* (June 2, 2016), *available at* https://www.ftc.gov/policy/policy-actions/advocacy-filings/2016/06/comment-staff-bureau-consumer-protection-office.

[23] 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.

One part of the Big Data phenomenon is the ease with which anyone can buy detailed data about consumers. We continue to focus on data brokers and, in particular, the role they play, wittingly or unwittingly, in facilitating fraud. Last year, I talked about our cases against data brokers that sold consumers' payday loan applications to fraudsters, and that posted detailed consumer debt information on the internet.[24] This year, we brought a similar case against data broker Sequoia One, which was able to purchase the payday loan applications of financial strapped consumers – including names, addresses, phone numbers, SSNs, and bank account numbers – and then sell them to scam artists who used the data to withdraw millions of dollars from consumers' accounts.[25] We also hosted a public workshop to examine the growing use of online lead generation in various industries, and to highlight best practices so lead generators can avoid becoming the next Sequoia One.[26] This continues to be an area of concern and, as I keep saying, Exhibit A in response to that big privacy question, "Where's the harm?"

Finally, another aspect of Big Data is the pervasiveness of online tracking. In November, we hosted a workshop on cross-device tracking to examine the various ways

[24] *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. Bayview Solutions LLC*, No. 1:14-cv-01830-RC (D.D.C. filed Oct. 31, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3226-x140062/bayview-solutions-llc; *FTC v. Cornerstone & Co.*, No. 1:14-cv-01479-RC (D.D.C. filed Aug. 27, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3211-x150005/cornerstone-company-llc.

[25] *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.

[26] FTC Workshop, *Follow the Lead: An FTC Workshop on Lead Generation* (Oct. 30, 2015), *available at* https://www.ftc.gov/news-events/events-calendar/2015/10/follow-lead-ftc-workshop-lead-generation.

that companies now track consumers across multiple devices, and not just within one device.[27] We expect to release an analysis of this workshop in the coming months.

Data Security

Data security also continues to be an important part of our privacy work. In August, in the *Wyndham* case, the Third Circuit affirmed our authority under the FTC Act to challenge data security failures, which we hope puts that issue to rest.[28] Soon after, we settled the Wyndham case in a fairly innovative way that built on, but substantially strengthened, the requirements in the existing Payment Card Industry standards.[29]

A lot of our recent work in data security has been educational – to stop breaches before they occur. Last year, we launched our *Start with Security* campaign to educate businesses, particularly small ones, about how to develop strong data security programs. As part of the campaign, we released new educational materials, including our guidance on the "lessons learned" from the FTC's 60 cases to date. We also hosted events around the country on security topics and best practices. Our next one is in Chicago next week.

In August, we also launched our new IdentityTheft.gov site, which makes it easier for consumers to report identity theft and take steps to remedy it.[30] Consumers can now use the site to manage and store their progress in the remediation process. We hope, in

[27] FTC Workshop, *Cross Device Tracking* (Nov. 16, 2015), *available at* https://www.ftc.gov/news-events/events-calendar/2015/11/cross-device-tracking.
[28] *FTC v. Wyndham Worldwide Corp.*, No. 14-3514 (3d Cir. Aug. 24, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/1023142-x120032/wyndham-worldwide-corporation.
[29] *FTC v. Wyndham Worldwide Corp.*, 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.
[30] FTC Press Release, *FTC Announces Significant Enhancements to IdentityTheft.gov*, Jan. 28, 2016, *available at* https://www.ftc.gov/news-events/press-releases/2016/01/ftc-announces-significant-enhancements-identitytheftgov.

the next phase, to link to the consumer reporting agencies in real time, but we are still working to get their cooperation in that process.

III. Research and Advocacy

Finally, I want to highlight our efforts to educate ourselves and the public about developments in the marketplace. One part of this effort is increasing the technological expertise of our staff. This year, we continued to expand the role of our Office of Technology Research and Investigations. OTech, as we call it, trains our staff about new technology and new investigative tools; helps plan and conduct our research and workshops; and hosts visiting scholars and interns to assist with the tech aspects of our mission. This year, we added a research director and research fellow to OTech's ranks.

We have many workshops planned for the summer and fall, and OTech is involved in all of them. These include our Fall Tech Series on the privacy issues raised by Ransomeware (September), Drones (October), and Smart TVs (December). We also have our FinTech Forum on Marketplace Lending (tomorrow) and Crowdfunding (fall 2016). And we're holding our second annual conference to highlight research on the consumer implications of privacy and tech issues – PrivacyCon – in January.[31]

Working with Lorrie Cranor, our Chief Technology Officer, we also just announced a fall workshop on testing the effectiveness of consumer disclosures.[32] You may be wondering "How many workshops can the FTC have on disclosures?" Well, it's

[31] FTC Event, *PrivacyCon* (Jan. 12, 2017), *available at* https://www.ftc.gov/news-events/events-calendar/2017/01/privacycon; *see also* FTC Event, *PrivacyCon* (Jan. 14, 2016), *available at* https://www.ftc.gov/news-events/events-calendar/2016/01/privacycon.

[32] FTC Workshop, *Putting Disclosures to the Test* (Sept. 15, 2016), *available at* https://www.ftc.gov/news-events/events-calendar/2016/09/putting-disclosures-test.

an important topic. This one is also different because it focuses on how to *test and evaluate* the effectiveness of disclosures to make sure consumers understand them and can use them in their decisionmaking. The workshop will explore these issues with respect many types of disclosures, including icons, product labels, and interactive tools.

As you also may know, we're also conducting a study of the security provided for mobile devices and we just issued requests for information to eight device manufacturers.[33] The FCC is conducting its own study of the carriers' role in mobile security, and both studies should yield interesting information about how these entities issue security updates to address vulnerabilities in smartphones, tablets, and other mobile devices.

Last but not least, part of our research agenda is advocacy to other agencies and I know our comment on the FCC's proposed broadband rule has generated a lot of interest. I understand Commissioner Ohlhausen will discuss the comment this afternoon, but I'd be happy to take questions about it.

IV. Conclusion

So that's a snapshot of our recent activities and some on the horizon too. We've been very active and I hope we've given everyone a lot to think about. Thank you for having me here today. I'm happy to take questions.

[33] Press Release, *FTC To Study Mobile Device Industry's Security Update Practices*, May 9, 2016, *available at* https://www.ftc.gov/news-events/press-releases/2016/05/ftc-study-mobile-device-industrys-security-update-practices.