Federal Trade Commission

Trends in Consumer Protection:
Issues Facing the FTC Today

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

NAD – Annual Conference 2016
September 26, 2016

Good morning. It's great to be here to discuss the consumer protection issues facing consumers and the FTC. NAD is one of our best partners and I know that many of you here today regularly engage with us and deal with the same consumer protection issues we do.

It should come as no surprise, then, that at the FTC, we take our cues from the marketplace. We closely monitor what's happening, evaluate how consumers are affected, and target our enforcement, policy, and educational efforts at practices most likely to undermine consumers' choices and do them harm.

These days, the market is giving us lots of cues. In the last few years, we've seen a number of trends that change the way consumers find information, shop and pay for goods and services, interact with businesses and friends, and access their cars, appliances, and thermostats with the press of a button.

Many of these changes involve technology, whether it comes in the form of new products and services; new ways that companies collect, use, analyze, and share consumer data; or new media to reach and communicate with consumers. These changes are altering every aspect of consumers' lives, and some of them are incredibly helpful and exciting. But they also raise new challenges for consumer protection.

One way we're responding to these changes is to educate ourselves and beef up our in-house technological expertise. Last year, we created our Office of Technology Research and Investigations, and we have steadily expanded its role at the agency. OTech, as we call it, trains our staff about new technology and investigative tools; helps plan and conduct our research and workshops; hosts visiting scholars and interns; and engages with the tech community. Increasingly, you'll see members of this team present research at FTC workshops, and publish papers on our website and elsewhere. Our goal is to protect consumers effectively in today's marketplace, and also to expand our role and identity as the nation's consumer protection agency for tech issues.

But the changes and challenges we face go well beyond one office. This morning, I'd like to provide an overview of some of the trends and issues we're dealing with across our program areas.

I. Advertising

Let's start with advertising. As you know, our advertising program maintains a steady diet of deceptive health and weight loss claims and deceptive disclosure practices. But three breakout themes we're dealing with right now are health apps, health claims that target aging consumers, and advertising in new media.

Deceptive Health Apps

Health apps and devices are just about everywhere. Just as consumers have migrated to the mobile platform for their email, music, and shopping, they're embracing the many mobile products that enable them to monitor and improve their health – apps to track their diet and exercise, devices to monitor their glucose levels, and social networks where consumers can share information with others who have the same health condition.

Many of these products and services are highly innovative and convenient, and some can be lifesaving. But as with other health products, they may also bring false claims to diagnose and cure illnesses and medical conditions, false or exaggerated claims about the studies and science behind the products, or health claims based on no substantiation at all. And sure enough, in the past couple of years, we've brought actions against apps that claimed to diagnose cancerous moles;[2] apps that promised to cure consumers' acne;[3] an app that claimed it could "turn back the clock" on consumers' vision through a series of visual exercises;[4] and an app and website that claimed its brain-training games could help users perform better at work or school, and reduce cognitive impairment associated with aging.[5] These products are on the rise, they raise serious concerns, and they're a growing part of our advertising program. The same rules of substantiation apply.

Health Products for Older Consumers

Speaking of cognitive impairment and "turning back the clock," another troubling trend we're seeing involves deceptive claims targeted at older consumers – clearly a profitable market segment as baby boomers age. Over the last two years, we've brought multiple cases against companies making unsupported claims that their products can stave off memory loss, cognitive impairment, dementia, and even Alzheimer's disease.[6]

And it's not just cognitive claims. We're also seeing unfounded claims that various products can relieve diabetes, heart disease, arthritis, insomnia, menopausal symptoms, and other ailments related to aging;[7] that supplements will eliminate grey hair at their roots,[8] and even that skin creams will alter women's genes and stimulate the production of youth proteins.[9] These types of claims – especially those involving serious medical conditions – remain a priority, and we have more in the pipeline.

New Media, New Formats

The last theme I want to highlight in the advertising area is the effect that new media and new formats are having on how consumers *receive* advertising. Screens are getting smaller and smaller. With the dominance of social media and online reviews, anyone can be a paid influencer or blogger, so knowing the source of information really counts. Ads look like content and vice versa. In this environment, we're particularly concerned about deceptive endorsements, native advertising, and ensuring that consumers actually see and understand important disclosures needed to prevent deception.

We've put out a lot of guidance on these topics,[10] but the basic principles are pretty simple. One is that consumers have a right to know when a supposedly objective opinion is actually a marketing pitch. That's why it was deceptive for Warner Brothers and Machinima not to make clear that they paid online influencers to post positive gameplay videos on social media;[11] for ADT not to make clear that the supposedly impartial experts reviewing its home security system on TV and radio were actually paid spokesmen;[12] for NourishLife to create a supposedly independent research site to tout its cure for childhood speech disorders;[13] and for Lord and Taylor[14] not to make clear that the magazine article on its clothing launch was really a paid promotion.[15]

A related principle is that companies can't use gag clauses and threats to undermine the integrity of online reviews intended to provide truthful, candid information to consumers. Last year, we sued *Roca Labs* for using a hidden gag clause and threats of suit to prevent consumers from posting negative reviews about its weight loss product, thus preventing the truth about the product from getting out.[16] We're looking carefully at gag clauses in other cases, and Congress is considering bills to ban them.

As consumers use mobile devices and media like Twitter with limited space and content, it's also becoming more and more challenging to provide them with meaningful disclosures. But it *can* be done, and we have terrific guidance to help, including our updated *Dot Com Disclosures* guide.[17] We also strongly encourage companies to experiment with icons and interactive tools to convey information simply and noticeably, and to test disclosures wherever possible to make sure they're effective.

Just two weeks ago, our Chief Technologist Lorrie Cranor and BCP hosted a workshop on testing disclosures, and it affirmed that testing can be critical to a disclosure's success.[18] But many participants also talked about new paradigms for disclosure, especially in the area of privacy, where many data practices now happen behind the scenes, hidden and seemingly tangential to the immediate transaction or decision the consumer is making. For example, we heard about research underway to develop apps and algorithms that will make privacy inferences and decisions for us, and tools to manage privacy choices all in one place. Lorrie and the team will soon post a blog on the workshop and next steps in this area.

In the coming months, we'll continue to focus on deceptive health claims and disclosure issues. On the disclosure front, upcoming events will include release of new research, and our October 6 workshop on how consumers interpret the term "organic."[19] On the health front,

they'll include the release of guidance on substantiation for homeopathic health claims, as a follow-up to last year's workshop. Stay tuned.

II. Privacy

Now I'd like to move to privacy and discuss some of the trends and issues we're dealing with there, too. Technology has obviously been a game-changer for privacy. Data collection, personalization and predictions, and round-the-clock tracking have just exploded – whether it's through your mobile device, Fitbit, smart car, social network, or thermostat. Much of this, as I mentioned, occurs behind the scenes and can involve dozens, even hundreds of companies that are invisible to consumers. And as we move further into the era of the Internet of Things, data collection will become even more ubiquitous and invisible.

These changes pose enormous challenges for consumers who want to understand and manage how their data is collected, used, and shared. Are they supposed to stop and read hundreds of privacy policies as they go about their day? Even if they tried, they'd fail, since they know nothing about most of the companies that gain access to their data.

Given the significant challenges consumers face in this area, we have our eyes on a wide range of issues, many of which involve deceptive or harmful data practices that consumers have little ability to detect or avoid on their own. In the last two years, for example, we've challenged deceptive data collection by mobile apps;[20] the deceptive tracking of customers in retail stores;[21] extortion and revenge-porn social media sites;[22] mobile ad networks that track consumers' location data without their consent;[23] tech companies that fail to provide basic security for mobile devices, apps, and software;[24] deceptive security claims by an identity theft protection company; [25] and the sale of sensitive consumer data to scam artists.[26] We've also hosted workshops on mobile device tracking, predictive scoring models, health apps,[27] and Big Data;[28]

we're in the midst of our Fall Tech Series on ransomware, drones, and smart TVs;[29] and we're planning another PrivacyCon to highlight research on tech and privacy issues.[30] Let me expand, in particular, on some key areas we're watching and what we're concerned about.

Internet of Things

First is the Internet of Things. It *has* arrived, it's expanding by leaps and bounds, 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 vast amounts of consumer data, some of it very personal.

One key issue is how to provide privacy information and choices to consumers in an environment where devices may be speaking to each other directly and there may not even be a screen for consumers to engage with. The answer is that companies need to innovate and adapt, and not leave consumer privacy behind. For example, you can provide choice at point of sale or during set-up and installation. You can use icons, codes, set-up wizards, and dashboards to communicate important privacy information and help consumers make choices.[31] Marketers can surely figure this out. At our recent disclosure workshop and last year's PrivacyCon, we heard research about new ways to provide information and choices, and we strongly support this ongoing work.

Another concern is data security. Two recent FTC cases illustrate what happens when IoT devices aren't secure – one against a security camera company whose poor security exposed live video feeds on the web,[32] and another against a leading router company whose poor security put consumers' data and home computer systems at risk.[33]

Device security – which can be distinct from data security – is a special concern for IoT devices. If hackers steal your data, it's bad. But if they hack and takeover your smart car, your

pacemaker, or your insulin pump, it's worse. And there's been evidence they can in some instances.[34] Given the seriousness of these risks and the rapid growth of IoT devices, we have a number of investigations underway in this area.

Health Privacy

Health privacy is also a priority. With consumers using health and fitness devices, researching their health issues online, and storing their health data electronically, the collection of health data and accompanying risks have just exploded in recent years. And because much of this activity now takes place outside of hospitals and doctors' offices, it's often 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.[35]

Health data is sensitive and personal, so we've been active in this area. For example, we recently challenged deceptive claims about doctor reviews by an e-health records company, which led to the public disclosure of consumers' names, medications, and health conditions;[36] deceptive encryption claims by the provider of dental office management software;[37] and the use of a deceptive sign-up process by a medical billing site to trick consumers into consenting to data sharing.[38] Because many companies operating in this space are small, we're also emphasizing business education. This year, we worked with HHS and the FDA to develop an interactive tool showing health app developers which laws apply to them,[39] and we released guidance to help them build privacy and security into their apps.[40] Health privacy will continue to be an area of concern.

The Privacy/Fraud Connection

Another concern is the increasing ability of scam artists to purchase sensitive data to aid in their frauds. Given the extensive data collection in today's marketplace, and the omnipresence

of data brokers and lead generators, it's easier and easier for anyone – including fraudsters – to purchase highly sensitive information about consumers, including account numbers and SSNs.

We've brought a number of cases highlighting the role that data brokers and lead generators have played in facilitating fraud.[41] We also held a workshop on lead generation, and followed up with a staff summary focusing on this issue.[42] The bottom line is that companies that sell sensitive consumer data should know who they're selling to, look for signs of fraud and deception, and avoid selling to anyone that doesn't have a legitimate need for the information.[43] Whenever we investigate a scam, we look for the scammer's source of leads.

Challenges

Finally, I want to call attention to some of the "big challenges" we face in protecting consumer privacy as we move further into the tech era. I've been working on privacy issues since the late 1990s, and in some respects, the issues remain the same: let's give consumers control of how their data is collected and used, and let's make sure that consumer data is secure when it's transmitted and stored. But technology is challenging some of the foundational thinking in this area. While it's given us more tools to protect consumers, it's also created infinite ways to collect, use, and share data, and infinite ways to evade the protections that consumers and companies put in place.

First, as I talked about with respect to the Internet of Things, it's become virtually impossible for consumers to manage their privacy through existing notice and choice mechanisms. Researchers are hard at work on apps and algorithms to help consumers. The FTC has also addressed this issue in its reports and policymaking – for example, recommending that companies offer consumers choices for data uses that are unexpected but not for routine, expected purposes.

I'm very proud of our work on this issue, but I do believe we need to move forward with some serious thinking about how use-based restrictions can help us here. If we could agree on a set of permissible and impermissible uses in certain discrete areas, maybe we could further simplify choices for consumers.

Another aspect of this challenge is that companies are now able to make predictions about consumers, or derive sensitive information about them, based on seemingly innocuous data. For example, one group of researchers was able to discern people's gender, sexuality, race, age, and political affiliation based solely on their Facebook likes,[44] and some companies reportedly use shopping history to determine consumers' credit risks and credit limits.[45] In this environment, it may be more meaningful to talk about sensitive *uses* of data, rather than sensitive data – again, pointing to the value of exploring use-based models as a *complement* to choice models.

A second, related issue I want to highlight is the breakdown of the traditional distinction between PII and non-PII. For several years now, the Commission has discussed the increasing ease with which companies use persistent identifiers to link data to a particular person or device, even if the company doesn't collect a name, address, SSN, etc. If you can use data to track and communicate with consumers, and you can figure out who they are with reasonable effort, the data should be treated and protected as PII. For this reason, our Privacy Report makes clear that companies should consider persistent identifiers to be PII if they can be reasonably linked to a particular person or device.[46] You *must* take this into account as you write your privacy policies and decide what level of protection to provide for your data.

A third challenge is that many of the threats we face, particularly on the data security front, come from overseas. This makes it harder for you, and for the FTC, to "deter, detect, and

defend" against dangers to systems and to data. We're building international frameworks to help address this issue. But this state of play reaffirms our view that the best defense is to secure one's own systems against the threats, and not to harbor hopes of stopping the threats themselves.

III. Other Significant Trends – FinTech, Every Community, Litigation

Finally, while I know this group is primarily interested in advertising and privacy, I do want to mention a few other trends that are driving the FTC's work. One is financial technology, or FinTech – technologies that enable consumers to store, share, and spend money in new ways. Yes, it's technology again. Our cases in this area have addressed such issues as unauthorized billing on kids' apps,[47] cramming charges on mobile phone bills,[48] false promises of unlimited data,[49] and fraud involving virtual currencies and crowdfunding.[50]

FinTech is a huge growth area for business, consumers, and the work of the FTC. It offers tremendous opportunities for consumers, but also raises questions about how these new forms of lending compare to conventional lending; which agencies have oversight; and whether new regulation will be needed in these areas. We're closely tracking developments – for example, by hosting our FinTech series this year on marketplace lending, crowdfunding, and peer-to-peer lending.[51] I urge you to tune into our next event on October 26.

Another trend we're closely following – and one that significantly affects our fraud program in particular – is the changing demographics in this country. We're getting older and more diverse. This diversity has significantly affected the types of frauds we see and the populations they target.

The FTC launched the *Every Community Initiative* in 2014 to examine the marketplace experiences of people in different communities – older Americans, African Americans, Latinos,

and military families, among others – and to identify and stop fraud and other harmful practices aimed at these consumers. This project includes outreach around the country with local enforcers, community groups, and ethnic media, and use of our strongest tool – enforcement – to protect these communities. We recently released a report to Congress on this project[52] and, in December, we're hosting a workshop to examine the effects of changing consumer demographics on the marketplace.[53]

Although the focus of this effort is mostly fraud, its impact is broader. For example, we're examining the consumer complaints we receive to figure out why certain groups complain to us and others don't, and how we can change that. And we're increasingly developing educational materials tailored to specific communities so they're more likely to read them. These may be good resources for some of your customers.

Finally, you may have noticed that during the last five to seven years, starting with my predecessor and expanding with me, the Bureau of Consumer Protection has become ever more focused on litigation, and being prepared to litigate large and complex cases if needed to obtain a strong result for consumers. This means there will be some losses but it also brings significant gains. And our readiness to litigate also can mean stronger settlements on the eve of litigation. I'd point you to Volkswagon, Herbalife, AT&T, T-Mobile, Wyndham, POM Wonderful, Apple, Amazon, Google, DirectTV, and Devry, among many others. I've made structural changes within BCP to strengthen the support we provide for litigation. And at every stage in the process – granting consent authority, meeting with counsel, forwarding a matter to the Commission – the key question is always "Are we ready to litigate this case?"

III. Conclusion

So, I'll conclude my prepared remarks on that macho note. As you can see, we're very busy in BCP on enforcement, policy initiatives, and spotting trends so we can get ahead of them. And I'd add that we know that NAD is busy too, monitoring the marketplace and pursuing self-regulation in a meaningful and accountable way, and we're very grateful for that. Thank you for having me here today – I look forward to answering any questions you have.

---

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

[2] *See 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] *See Koby Brown & d/b/a Dermapps, et al.*, No. C-4337 (Oct. 25, 2011), *available at* https://www.ftc.gov/enforcement/cases-proceedings/102-3205/brown-koby-individually-dba-dermapps-et-al-matter; *Andrew N. Finkel*, No. C-4338 (Oct. 25, 2011), *available at* https://www.ftc.gov/enforcement/cases-proceedings/102-3206/finkel-andrew-n-individually.

[4] *See 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.

[5] *See FTC v. Lumos Labs, Inc.*, 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.

[6] *See, e.g., FTC v. LearningRx Franchise Corp.*, No. 1:16-cv-01159-RM (D. Colo. May 24, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3206/learningrx-franchise-corp; *FTC v. Brain Research Labs, LLC*, No. 8:15-cv-01047 (C.D. Cal. filed July 8, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3242/brain-research-labs-llc; *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; *i-Health, Inc. & Martek Biosciences Corp.*, No. C-4486 (Aug. 21, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3067/i-health-martek-matter.

[7] *See, e.g., Genelink, Inc.*, No. C-4456 (May 12, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3095/genelink-inc-matter; *foru Int'l Corp.*, No. C-4457 (May 12, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3095/forutm-international-corporation-matter.

[8] *See FTC v. COORGA Nutraceuticals Corp.* No. 15-CV-72-S (D. Wy. Sept. 23, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3119-x150037/coorga-nutraceuticals-corp-grey-defence; *FTC v. Rise-N-Shine, LLC*, No. 15-3301 (D.N.J. May 20, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3095/rise-n-shine-llc-go-away-gray; *FTC v. GetAwayGrey, LLC*, No. 2: 15-cv-1990-RMG (D.S.C. May 14, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3097/getawaygrey-llc.

[9] *See L'Oreal USA, Inc.*, No. C-4489 (Sept. 26, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3016/loreal-usa-matter.

[10] *See, e.g., 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.

[11] *See Warner Bros. Home Entertainment, Inc.*, Matter No. 1523034 (July 11, 2016) (proposed consent), *available at* https://www.ftc.gov/enforcement/cases-proceedings/152-3034/warner-bros-home-entertainment-inc-matter; *Machinima, Inc.*, No. C-4569 (Mar. 17, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3090/machinima-inc-matter.

[12] *ADT LLC*, No. C-4460 (June 18, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3121/adt-llc-matter; *see also FTC v. Genesis Today, Inc. et al.*, 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.

[13] *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.

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

[15] *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.

[16] *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.

[17] *Dot 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. *See also Mobile Privacy Disclosures: Building Trust Through Transparency* (Feb. 2013), *available at* https://www.ftc.gov/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission.

[18] 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.

[19] *Consumer Perceptions of "Organic" Claims: An FTC and USDA Roundtable Discussion of Evidence Concerning Particular Issues* (Oct. 20, 2016), *available at* https://www.ftc.gov/news-events/events-calendar/2016/10/consumer-perceptions-organic-claims-ftc-usda-roundtable.

[20] *See, e.g., Snapchat, Inc.*, No. C-4501 (Dec. 23, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3078/snapchat-inc-matter; *Goldenshores Technologies, LLC*, No. C-4446 (Mar. 31, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3087/goldenshores-technologies-llc-erik-m-geidl-matter.

[21] *See Nomi Technologies, Inc.*, No. C-4538 (Sept. 3, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3251/nomi-technologies-inc-matter.

[22] *See Craig Brittain*, No. C-4564 (Jan. 8, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3120/craig-brittain-matter; *Jerk, LLC*, Docket No. 9361 (Mar. 13, 2015) (summary judgment decision), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3141/jerk-llc-dba-jerkcom-matter.

[23] *See U.S. v. InMobi Pte Ltd.*, No. 3:16-cv-03474 (N.D. Cal. filed June 22, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/152-3203/inmobi-pte-ltd.

[24] *See, e.g., Oracle Corp.*, No. C-4571 (Mar. 29, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3115/oracle-corporation-matter; *Credit Karma, Inc.*, No. C-4480 (Aug. 13, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3091/credit-karma-inc; *Fandango, LLC*, No. C-4481 (Aug. 13, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3089/fandango-llc; *HTC America, Inc.*, No. C-4406 (June 25, 2013), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3049/htc-america-inc-matter.

[25] *See FTC v. Lifelock*, No. CV-10-00530-PHX-JJT (D. Az Dec. 17, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/072-3069-x100023/lifelock-inc-corporation.

[26] *See FTC v. Sitesearch Corp., LLC*, No. CV-14-02750-PHX-NVW (D. Az. Feb 5, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3192/sitesearch-corporation-doing-business-leaplab; *FTC v. Sequoia One, LLC*, No. 2:15-cv-01512-JCM-CWH (D. Nev. filed Aug. 12, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3253/sequoia-one-llc.

[27] Press Release, *FTC to Host Spring Seminars on Emerging Consumer Privacy Issues* (Dec. 2, 2013), *available at* https://www.ftc.gov/news-events/press-releases/2013/12/ftc-host-spring-seminars-emerging-consumer-privacy-issues.

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

[29] Press Release, *FTC to Host Fall Seminar Series on Emerging Consumer Technology Issues* (Mar. 31, 2016), *available at* https://www.ftc.gov/news-events/press-releases/2016/03/ftc-host-fall-seminar-series-emerging-consumer-technology-issues.

[30] *PrivacyCon* (Jan. 12, 2017), *available at* https://www.ftc.gov/news-events/events-calendar/2017/01/privacycon.

[31] *See* 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.

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

[33] *See ASUSTeK Computer Inc.*, No. C-4587 (July 28, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3156/asustek-computer-inc-matter.

[34] *See, e.g.*, Charlie Miller & Chris Valasek, *Remote Exploitation of an Unaltered Passenger Vehicle* (2015), *available at* http://illmatics.com/Remote%20Car%20Hacking.pdf.

[35] 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).

[36] *See 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.

[37] *See 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.

[38] *See PaymentsMD, LLC*, No. C-4505 (Jan. 27, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3088/paymentsmd-llc-matter.

[39] *See* Mobile Health Apps Interactive Tool (Apr. 2016), *at* https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool.

[40] *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.

[41] *See, e.g.*, *FTC v. Expand, Inc.*, No. 6:16-cv-00714-CEM-TBS (M.D. Fl. Sept. 15, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/152-3124/expand-inc-gigats; *FTC v. Sitesearch Corp., LLC*, No. CV-14-02750-PHX-NVW (D. Az. Feb 5, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3192/sitesearch-corporation-doing-business-leaplab; *FTC v. Sequoia One, LLC*, No. 2:15-cv-01512-JCM-CWH (D. Nev. filed Aug. 12, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3253/sequoia-one-llc.

[42] 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; FTC Staff Perspective, *"Follow the Lead" Workshop* (Sept. 2016), *available at* https://www.ftc.gov/reports/follow-lead-workshop-staff-perspective.

[43] FTC Staff Perspective, *"Follow the Lead" Workshop* (Sept. 2016), *available at* https://www.ftc.gov/reports/follow-lead-workshop-staff-perspective.

[44] *See* Rebecca J. Rosen, *Armed With Facebook 'Likes' Alone, Researchers Can Tell Your Race, Gender, and Sexual Orientation*, THE ATLANTIC (Mar. 12, 2013), *available at* http://www.theatlantic.com/technology/archive/2013/03/armed-with-facebook-likes-alone-researchers-can-tell-your-race-gender-and-sexual-orientation/273963/.

[45] *See* Ron Lyber, American Express Kept a (Very) Watchful Eye on Charges, N.Y. TIMES (Jan. 30, 2009), *available at* http://www.nytimes.com/2009/01/31/your-money/credit-and-debit-cards/31money.html?hp&_r=0.

[46] *See also* Children's Online Privacy Protection Act ("COPPA") Rule, 16 C.F.R. Part 312.

[47] *See FTC v. Amazon.com*, No. 2:14-cv-01038 (W.D. Wash. Apr. 27, 2016) (summary judgment decision), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3238/amazoncom-inc; *Google, Inc.*, No. C-4499 (Dec. 2, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-

3237/google-inc; *Apple, Inc.*, No. C-4444 (Mar. 25, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3108/apple-inc.

[48] *See FTC v. T-Mobile USA, Inc.*, No. 2:14-cv-0097-JLR (W.D. Wash. filed Dec. 19, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3231/t-mobile-usa-inc.; *FTC v. AT&T Mobility, Inc.*, No. 1:14-cv-3227-HLM (N.D. Ga. filed Oct. 8, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3248/att-mobility-llc

[49] *See FTC v. TracFone Wireless, Inc.*, No. 3:15-cv-00392 (N.D. Cal. filed Jan. 28, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3176/straight-talk-wireless-tracfone-wireless-inc.

[50] *See FTC v. BF Labs, Inc.*, No. 4:14-cv-00815-BCW (W.D. Mo. Feb. 18, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3058/bf-labs-inc; *FTC v. Equiliv Investments*, Matter No. 142-3144 (D.N.J. filed June 29, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3144/equiliv-investments-prized; *FTC v. Erik Chevalier, Co.*, No. 3:15-cv-1029-AC (D. Ore. filed June 11, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3061/erik-chevalier-forking-path.

[51] FinTech Series, *Crowdfunding & Peer-to-Peer Payments*, Oct. 26, 2016, *available at* https://www.ftc.gov/news-events/events-calendar/2016/10/fintech-series-crowdfunding-peer-peer-payments; FinTech Series, *Marketplace Lending*, June 9, 2016, *available at* https://www.ftc.gov/news-events/events-calendar/2016/06/fintech-series-marketplace-lending.

[52] FTC Report to Congress, *Combating Fraud in African American and Latino Communities: The FTC's Comprehensive Strategic Plan* (June 2016), *available at* https://www.ftc.gov/reports/combating-fraud-african-american-latino-communities-ftcs-comprehensive-strategic-plan.

[53] *See* FTC Workshop, *Changing Consumer Demographics* (Dec. 6, 2016), *available at* https://www.ftc.gov/news-events/events-calendar/2016/12/changing-consumer-demographics.