Federal Trade Commission

FTC 2016 – Meeting the Challenges of the Digital Revolution

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

WOMMA – October 6, 2015

Good morning. This is the first time I have spoken at a WOMMA event and I'm delighted to be here. Today, I'm going to talk about the FTC's recent work to protect consumers – and in particular, how the FTC is meeting the challenges posed by the digital revolution.

Everyone in this room knows that technology has been a game-changer for the marketplace. From Facebook to YouTube, from text messages to tweets, the digital revolution has fundamentally altered how companies communicate and engage with consumers.

Consumers have benefitted enormously from this explosive growth. The surge in the use of smartphones and connected devices enables consumers – from any location – to find information, contact friends, shop and pay for goods and services, update their social networks, monitor their health and fitness, and access devices in their cars and homes remotely.

But these changes also pose immense challenges for consumer protection. Today, commerce comes at us from every direction, at every minute – through the smartphones we carry

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

with us everywhere and the many other connected devices that are all around us. Data-driven predictions about who we are and what we will do determine the information we receive and the offers we get. And, increasingly, consumers themselves become the marketers, as they're enlisted in campaigns on social media to tout products and services to friends and acquaintances.

Adding to these challenges, many of the technologies that drive our daily lives now have small screens or no screens at all. And many of the companies that receive and use our personal information are behind the scenes, unknown to us. As a result, it's harder to rely on some of the traditional tools we have used to protect consumers – disclosures to avoid deception, privacy policies to describe data practices, and the basic notion that consumers can make meaningful choices about who they do business with.

The FTC has made significant shifts in its consumer protection agenda to address these challenges. This is what I plan to talk about this morning. In particular, I'm going to focus on how to the FTC is addressing the explosive growth of new technologies across our range of programs – including privacy, deceptive advertising, and basic fraud. .

Our goal is to make clear that the fundamental principles of consumer protection still apply to today's marketplace. Yes, they need to be adapted and updated. But the basic rules still apply: Tell the truth. Disclose any facts necessary to make sure your claims aren't 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 timeless, and we expect companies to abide by them across all of their business models – old and new.

I. Mobile and New Technologies

Nowhere are the effects of the digital revolution more dramatic than in privacy. But I'm going to set privacy aside for a moment so I can talk about some areas that may be less obvious, but nevertheless are transforming how consumers interact with the commercial marketplace.

Mobile Payments

With the growth of mobile payments, it has become easier for consumers to pay for goods and services instantly, with no messy paperwork. But these conveniences also make it easier for scam artists to commit fraud through mobile devices, and for consumers to incur unauthorized charges without noticing them.

Consumers shouldn't be charged for purchases they didn't authorize – period. We've emphasized this principle in dozens, even hundreds of FTC cases over the years – most recently in a series of cases involving mobile payments. For example, last year, we took action against Apple, Amazon, and Google[2] for allegedly failing to obtain parents' permission before letting kids run up charges in mobile gaming apps. So far, we've obtained over $50 million in consumer refunds from these cases; we hope to obtain even more once we resolve our case against Amazon.

We also took action against numerous companies – including (with all 50 states and the Federal Communications Commission) T-Mobile and AT&T[3] for allegedly "cramming"

---

[2] *Apple, Inc.*, No. C-4444 (Mar. 25, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3108/apple-inc; *FTC v. Amazon.com*, No. 2:14-cv-01038 (W.D. Wash. filed July 10, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3238/amazoncom-inc; *Google, Inc.*, No. C-4499 (Dec. 2, 2014) (F.T.C. consent), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3237/google-inc.

[3] *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.

unauthorized third-party charges on consumers' mobile phone bills.[4] Collectively, we've obtained over $160 million in consumer refunds from these cases. These actions make clear that companies offering new products and services on the mobile platform must also offer basic safeguards to prevent fraud and misuse.[5]

Deceptive Health Apps

We're also tackling unsubstantiated health claims on the mobile platform – and there are many. These claims can actually be dangerous if unproven products are touted as a substitute for medical care. For example, the FTC recently charged two app developers with deceptively claiming that their apps – Mole Detective and MelApp – could detect symptoms of melanoma, even in the early stages.[6] In fact, we alleged, the companies lacked evidence to show their apps could detect melanoma, early or at all. And most recently, we took action against an app called

[4] *See also FTC v. Jesta Digital LLC*, No. 1:13-cv-01272 (D.D.C. filed Aug. 20, 2013), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3187/jesta-digital-llc-also-dba-jamster; *FTC v. Wise Media LLC*, No. 113-CV-1234 (N.D. Ga. filed Apr. 17, 2013), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3182/wise-media-llc-et-al; *FTC v. Tatto, Inc.*, No. 2:13-cv-08912-DSF-FFM (C.D. Cal. filed Dec. 5, 2013), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3181/tatto-inc-also-dba-winbigbidlow-tatto-media-et-al.

[5] To explore and address this and other consumer protection issues raised by the growing use of mobile payments, the Commission has held workshops and issued reports. *See, e.g.*, FTC Staff Report, *Mobile Cramming: An FTC Staff Report* (July 2014), *available at* https://www.ftc.gov/system/files/documents/reports/mobile-cramming-federal-trade-commission-staff-report-july-2014/140728mobilecramming.pdf; FTC Staff Report, *What's the Deal?: An FTC Study on Mobile Shopping Apps* (Aug. 2014), *available at* https://www.ftc.gov/reports/whats-deal-federal-trade-commission-study-mobile-shopping-apps-august-2014.

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

Ultimeyes, which claimed to have scientific proof that it could "turn back the clock" on consumers' vision through a series of visual exercises.[7] In fact, we alleged it had no such proof.

Fraud on New Platforms

Scam artists also are exploiting new platforms to defraud consumers in new ways. For example, last year, we settled a series of cases cracking down on affiliate marketers[8] that we alleged bombarded consumers with hundreds of millions of unwanted text messages in an effort to steer them towards deceptive websites falsely promising "free" gift cards.[9]

---

[7] *Carrot Neurotechnology, Inc.*, No. 142 3132 (Sept. 17, 2015) (proposed consent order), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3132/carrot-neurotechnology-inc-matter-ultimeyes.

[8] *See FTC v. Advert Marketing Inc.*, No. 413-cv-00590 (S.D. Tex. stipulated order filed June 9, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3019-x130037/advert-marketing-inc-scott-dalrymple-robert-jerrold; *FTC v. Jason Q. Cruz, Inc.*, No. 1:13-cv-01530 (N.D. Ill. stipulated order filed Jan. 16, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3051-113-cv-01530/cruz-jason-q-also-dba-appidemic-inc; *FTC v. Ecommerce Merchants LLC.*, No. 113-cv-01534 (N.D. Ill. stipulated order filed Nov. 12, 2013), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3048/ecommerce-merchants-llc-dba-superior-affiliate-management-et; *FTC v. Henry Nolan Kelly*, No. 113-cv-00647 (N.D. Ga. stipulated order filed July 17, 2013), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3057/kelly-henry-nolan; *FTC v. Rentbro, Inc.*, No. 113-cv-01529 (N.D. Ill. stipulated order filed Sept. 13, 2013), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3049/rentbro-inc-daniel-pessin-jacob-engel; *FTC v. SubscriberBASE Holdings, Inc.*, No. 113-cv-01527 (N.D. Ill. stipulated order filed Feb. 6, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3137/subscriberbase-holdings-inc-et-al; *FTC v. Verma Holdings, LLC*, No. 4:13-cv-00594 (S.D. Tex. stipulated order filed July 15, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3018/verma-holdings-llc-rishab-verma.

[9] Even debt collectors are getting in on the texting act. In the past two years, we've taken action against a number of collectors that sent unwanted texts to deceive and threaten consumers. *See, e.g.*, *FTC v. Primary Group Inc.*, No. 1:15-CV-1645 (N.D. Ga. filed May 21, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/1423158/primary-group; *FTC v. Unified Global Group, LLC*, No. 1:15-cv-00422-EAW (W.D.N.Y. filed May 21, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/1423140/unified-global-group; *FTC v. Premier Debt Acquisitions LLC*, No. 1:15-cv-00421-FPG (W.D.N.Y. filed May 21, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/1423157/premier-debt-acquisitions; *U.S. v. National Attorney Collection Services, Inc.*, No. 2:13-cv-06212-ODW-VBK (C.D. Cal. filed Aug. 23, 2013), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3032/national-attorney-collection-services-inc.

More recently, we brought our first case involving the Kickstarter crowdfunding platform, against the creator of a project called Forking Path.[10] We alleged that the defendant used Kickstarter to raise money to produce a board game, telling backers they would get copies of the game and other rewards. After raising over three times his stated goal, he cancelled the project and promised to refund backers' money. In fact, we alleged, backers never got refunds because he spent the money on personal items such as rent, home equipment, and moving to Oregon.

We also recently took action against *Prized*, a mobile gaming app that supposedly earned consumers rewards.[11] The app promised it would be free from malware, but instead loaded consumers' mobile phones with malicious software to mine virtual currencies for the developer.

Deception in New Media

Technological developments also have led to dramatic changes in how consumers *receive* advertising. Today, everyone's a salesman – the doctor on TV, the blogger you follow, your friends on Facebook and, increasingly, the author of that seemingly authoritative article on the latest medical "breakthrough." We're living in an era where the line between advertising and objective content is increasingly blurry and confusing.

But sometimes, it's not just confusing – it's deceptive and illegal. We're particularly concerned about deceptive endorsements and fake news sites. The governing principle is pretty simple: Consumers have a right to know if an opinion or supposed "proof" is actually a marketing pitch.

---

[10] *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.

[11] *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; *see also FTC v. BF Labs, Inc.*, No. 4:14-cv-00815-BCW (W.D. Mo. filed Sept. 23, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3058/bf-labs-inc (alleging that the company deceptively marketed computers designed to produce Bitcoins).

We've made this point in numerous enforcement actions over the past two years. For example, in one of our cases challenging the slimming effects of "pure green coffee bean extract" (GCBE), we charged defendant Lindsey Duncan with passing himself off as an independent expert when he touted the supplement on the *The Dr. Oz Show*.[12] In fact, we charged, he was actually selling the supplement, deceptively, through websites he set up beforehand. In another, we alleged that marketer NPB Advertising set up fake news sites that made false claims about the effectiveness of GCBE and channeled people to another site where they could buy it.[13]

One particularly troubling case this year involved NourishLife, the marketer of a supplement for kids. We alleged that the company posted a fake research site, and trumpeted paid endorsements from parents, making unsubstantiated claims that the supplement was scientifically proven to treat childhood speech and behavioral disorders, including those associated with autism.[14] According to our complaint, it wasn't.

And just today, we filed a case in federal court alleging that Roca Labs not only promoted unproven weight loss supplements, but also threatened to sue – and did sue –

---

[12] *See 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.
[13] *FTC v. NPB Advertising, Inc.*, No. 8:14-cv-0155-SDM-TGW (M.D. Fla. filed May 15, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3116/npb-advertising-inc-et-al.
[14] *FTC v. NourishLife, LLC*, No. 1:15-cv-00093 (N.D. Ill. filed Jan. 7, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3152/nourishlife-llc. *See also FTC v. Lunada Biomedical, Inc.*, No. 2:15-cv-03380-MWF (PLAx) (C.D. Cal. filed May 12, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3067/lunada-biomedical-inc (alleging among other things that the supposedly independent bloggers recommending their supplements for weight loss and menopause symptoms were actually paid to do so); *FTC & Connecticut v. Leanspa, LLC*, No. 311-cv-01715 (D. Conn. Apr. 6, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/1123135/leanspa-llc-et-al (FTC and State of CT obtained $11.9 million judgment against affiliate marketing network LeadClick for using fake news sites to convince people that acai berry and colon cleansing weight loss products were proven effective).

consumers who posted negative reviews online, thus preventing the truth about the product from getting out.[15]

Unfortunately, these strategies have gained traction among more mainstream companies too. For example, last November, in connection with our action against Sony for deception claims about its gaming consoles,[16] we alleged that a manager at its ad agency, Deutsch, had directed employees to post positive tweets about the console as part of the Sony ad campaign.[17] And earlier this month, we charged Machinima, an entertainment network that worked for Microsoft's ad agency, with paying a large group of "influencers" to develop and post videos online touting XboxOne. [18] The videos appeared to be the objective views of the influencers, and did not disclose that the influencers were actually paid to tout the product.

The FTC's Endorsement Guides and FAQs provide detailed guidance about how to avoid this type of deception, including in newer forms of promotion like Twitter, affiliate marketing, "like" buttons, employee endorsements, and videos.[19] In general, when there are material connections (like payment) between a marketer and an endorser, they must be disclosed clearly

---

[15] *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.

[16] *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.

[17] *Deutsch LA, Inc.*, No. C-4515 (Mar. 24, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3252/deutsch-la-inc-matter. *See also AmeriFreight, Inc.*, No. C-4518 (Apr. 13, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3249/amerifreight-inc-matter (shipment broker failed to disclose that it provided discounts and awards to customers who posted online reviews of its service); *ADT LLC*, No. C-4460 (June 18, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3121/adt-llc-matter (home security company paid endorsers to tout products on NBC's *Today Show* and in other national media).

[18] *Machinima, Inc.*, No. 142 3090 (Sept. 2, 2015) (proposed consent order), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3090/machinima-inc-matter.

[19] *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. *See also 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.

and prominently. Promotional messages also must be identifiable as advertising – if not through their look and feel, then through a disclosure. This issue remains a priority and we plan to issue guidance on the issue of "native advertising" by the end of the year.[20]

Deceptive Broadband and Cable Claims

With everyone moving to mobile and cable, competition among service providers is fierce. But that doesn't excuse deceptive claims. Last year, we took action against wireless providers AT&T (yes, again) and TracFone for advertising "unlimited" data in their broadband plans when in fact, they slowed down (or "throttled") service when consumers reached a certain limit.[21] Unlimited means unlimited – it's a pretty straightforward word. TracFone paid $40 million in refunds to consumers; we're still in litigation with AT&T.

We also sued DirecTV for misrepresenting the costs of its cable service – including by failing to disclose that its contracts required a two-year commitment and that the price would be substantially higher than advertised in the second year.[22] We're in litigation with DirecTV, too.

Illegal Robocalls

Another priority area is robocalls. We receive about 300,000 Do Not Call complaints per month – 60% of which involve robocalls. Most robocalls are illegal unless the marketer has the prior written authorization from the consumer to make such calls. In recent years, technological

---

[20] *See* FTC Workshop, *Blurred Lines: Advertising or Content?*, Dec, 4, 2013, *available at* https://www.ftc.gov/news-events/events-calendar/2013/12/blurred-lines-advertising-or-content-ftc-workshop-native.

[21] *FTC v. AT&T Mobility, Inc.*, No. 14-cv-04785-EMC (N.D. Cal. filed Oct. 28, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3253/att-mobility-llc-mobile-data-service; *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.

[22] *FTC v. DirecTV*, No. 3:15-cv-01129 (N.D. Cal. filed Mar. 11, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/102-3141/directv.

changes have led to an explosion of these calls, which violate consumers' privacy and also provide a cheap vehicle to peddle fraud.

To date, the FTC has brought more than a hundred lawsuits against nearly 700 companies and individuals responsible for billions of illegal robocalls and other Do Not Call violations. Just this spring, we (along with 10 state attorneys general) took action against Carribbean Cruise Line and seven other companies engaged in a massive robocalling campaign to sell cruise vacations illegally, using deceptive political calls.[23] And this summer, we filed a joint complaint with the Florida AG alleging that defendant Lifewatch used illegal and deceptive robocalls to trick older consumers into signing up for medical alert systems with monthly monitoring fees.[24]

We also educate consumers about what they should do if they get unwelcome robocalls – basically, hang up and file a complaint with the FTC. And, we're leading several initiatives to develop technology-based solutions. These initiatives include a series of contests challenging tech gurus to design tools to block robocalls and help investigators track down and stop the people behind them. In August, we announced the winner of the FTC's latest robocall challenge.[25] We hope that with the assistance of products like Robokiller, a mobile app that blocks and forwards robocalls to a crowd-sourced honeypot, we can help consumers block billions of unwanted robocalls and report illegal robocallers to law enforcement.

I want to add that the FTC continues to prioritize enforcement of Do Not Call beyond robocalls. For example, in December, a federal court found Dish Network liable for tens of

---

[23] *FTC v. Caribbean Cruise Line, Inc.*, No. 0:15-cv-60423 (S.D. Fla. Mar. 4, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3196/caribbean-cruise-line-inc.
[24] *FTC v. Lifewatch, Inc.*, No. 1:15-cv-05781 (N.D. Ill. July 6, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3123/lifewatch-inc.
[25] Press Release, *FTC Awards $25,000 Top Cash Prize for Contest-Winning Mobile App That Blocks Illegal Robocalls* (Aug. 17, 2015), *available at* https://www.ftc.gov/news-events/press-releases/2015/08/ftc-awards-25000-top-cash-prize-contest-winning-mobile-app-blocks.

millions of calls that violated the FTC's Telemarketing Sales Rule, including Do Not Call.[26] The case goes to trial in January.

Office of Technology Research and Investigations

Lastly, 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, I created the Mobile Technology Unit (MTU) to help bring consumer protection into the mobile era. The MTU assisted BCP staff with law enforcement investigations. It also developed surveys on kids' apps, mobile shopping apps, and health apps.[27] This year, BCP announced that it 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 hiring more researchers and technologists.[28] 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.

II. Privacy and Big Data

That's a nice transition to privacy and Big Data. The effects of technology on privacy can't be overstated. Today, data is collected from consumers wherever they go – online, offline, through mobile and connected devices, everywhere. As I mentioned, most of the companies that collect consumers' data 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.

---

[26] *U.S. v. Dish Network, LLC*, No. 09-3073 (C.D. Ill. Dec. 12, 2014) (opinion), *available at* https://www.ftc.gov/enforcement/cases-proceedings/052-3167/dish-network-llc-united-states-america-federal-trade. *See also FTC v. Centro Natural Corp.*, No. 14:23879-CIV-ALTONAGA/O'Sullivan (S.D. Fla. July 8, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3159/centro-natural-corp (fraudulent debt collection operation violated Do Not Call).

[27] *See generally* https://www.ftc.gov/news-events/media-resources/mobile-technology.

[28] *See, e.g.*, Jessica Rich, *BCP's Office of Technology Research and Investigation: The Next Generation in Consumer Protection*, FTC Business Blog, Mar. 23, 2015, *at* https://www.ftc.gov/news-events/blogs/business-blog/2015/03/bcps-office-technology-research-investigation-next.

The use of data, and 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, again, is that even in the face of rapidly changing technology and business models, companies still need to follow the basic principles. In privacy, these include: don't collect or retain more data than you reasonably need. If you must collect data, de-identify it wherever possible. Protect data from unauthorized access. Give consumers accurate information and meaningful choices about their privacy. As new business models and technologies develop, these principles remain as important as ever, although they do need to be adjusted and adapted. We've emphasized these principles through enforcement, policy initiatives, and education.

Our enforcement actions include last year's case against mobile messaging app Snapchat. Among other things, Snapchat promised that the photos and videos sent through its app would disappear at a time set by the sender.[29] In fact, we alleged that recipients could use easy workarounds to keep the messages forever. We also took action against the maker of a popular flashlight app for misrepresenting that it would only collect data from users' devices for certain

[29] *Snapchat, Inc.*, No. C-4501 (Dec. 23, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3078/snapchat-inc-matter.

internal housekeeping purposes.[30] In fact, we alleged, it collected – and transmitted to third party ad networks – the device's location and device ID.

More recently, we addressed the growing practice by retailers of using mobile technologies to track the movements of their customers in stores. We alleged that Nomi Technologies, the analytics firm that performed these services, told consumers they would be notified when stores were using its tracking services and would be able to opt out then and there.[31] In fact, consumers weren't told at stores and couldn't opt out.

Health data is another important FTC concern because it's sensitive and often regarded as private. Also, HIPAA doesn't protect health data unless it's collected by a medical provider. But the FTC Act does. In December, we charged Payments MD, a health billing company, with using a deceptive registration process to trick thousands of consumers who signed up for its online billing portal into also consenting to collection of their detailed medical information from pharmacies, medical labs, and insurance companies.[32]

Then there are extortion 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, 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.[33] He then used another site to pose as an attorney and charge $250 for removing the information. The Commission also

---

[30] *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.

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

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

[33] *Craig Brittain*, Matter No. 132-3120 (Jan. 29, 2015) (proposed consent agreement), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3120/craig-brittain-matter.

issued a unanimous summary decision finding law violations by Jerk.com.[34] That case involved photos of kids and teens being labeled a "jerk," supposedly by their peers.

We've also brought numerous actions against companies that failed to implement reasonable protections for sensitive data – indeed, over 50 during the last 15 years.[35] Last year, for example, we brought our first case involving the Internet of Things. We alleged that video monitoring company TRENDnet failed to provide reasonable security for IP cameras used for home security and baby monitoring, which resulted in hackers posting private video feeds of people's bedrooms and children's rooms on the Internet.[36]

We also brought several cases involving mobile device security – including against mobile device manufacturer HTC for failing to secure its mobile devices,[37] and against mobile apps Credit Karma[38] and Fandango[39] for disabling a critical default process necessary to ensure that apps' communications were secure.

Other recent data security cases include actions against service provider Accretive Health,[40] supplement companies Genelink[41] and Genewize,[42] medical transcriber GMR

---

[34] *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.
[35] *See, e.g.*, *Commission Statement Marking the FTC's 50th Data Security Settlement*, Jan. 31, 2014, *available at* https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.
[36] *TRENDnet, Inc.*, No. C-4426 (Jan. 16, 2014), *available at* http://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter.
[37] *HTC America, Inc.*, No. C-4406 (June 25, 2013), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3049/htc-america-inc-matter.
[38] *Credit Karma, Inc.*, No. C-4480 (Aug. 13, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3091/credit-karma-inc.
[39] *Fandango, LLC*, No. C-4481 (Aug. 13, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3089/fandango-llc.
[40] *Accretive Health, Inc.*, No. C-4432 (Feb. 5, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3077/accretive-health-inc-matter.
[41] *Genelink, Inc.*, No. C-4456 (May 8, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3095/genelink-inc-matter.
[42] *foru Int'l Corp.*, No. C-4457 (May 8, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3095/forutm-international-corporation-matter.

Transcription Services,[43] and debt brokers Bayview[44] and Cornerstone.[45] And we have ongoing litigation against Wyndham Hotels[46] and LabMD[47] – and a contempt action against Lifelock[48] – for alleged failures to protect sensitive financial and health data. In *Wyndham*, the Third Circuit recently reaffirmed the FTC's authority under Section 5 to hold companies accountable for security failures.

This year, we are emphasizing our data security educational tools and taking our message on the road with our *Start with Security* campaign.[49] It includes events around the country on security topics and best practices. We just completed our first conference in San Francisco and we are gearing up for our next one in Austin on November 6. We also continue to put out new business guidance, including our latest piece on lessons learned from FTC data security cases.[50]

Additionally, we are vigorously enforcing the laws protecting the privacy and accuracy of sensitive consumer report data, [51] kids' privacy,[52] and data protected by the U.S.-EU Safe Harbor Framework.[53]

---

[43] *GMR Transcription Servs., Inc.*, No. C-4482 (Aug. 14, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3095/gmr-transcription-services-inc-matter.
[44] *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.
[45] *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.
[46] *FTC v. Wyndham Worldwide Corp.*, Civil No. 13-1887 (ES) (D.N.J. Apr. 7, 2014) (opinion denying defendant's motion to dismiss), *available at* http://www.ftc.gov/enforcement/cases-proceedings/1023142/wyndham-worldwide-corporation.
[47] *LabMD Inc.*, Docket No. 9357 (filed Aug. 28, 2013), *available at* https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter.
[48] *FTC v. Lifelock Inc.*, No. 2:10-cv-00530-MHM (D. Az. filed July 21, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/072-3069-x100023/lifelock-inc-corporation.
[49] *See* FTC Press Release, *FTC Kicks Off "Start with Security" Business Education Initiative*, June 30, 2015, *available at* https://www.ftc.gov/news-events/press-releases/2015/06/ftc-kicks-start-security-business-education-initiative.
[50] *Start with Security: A Guide for Business* (June 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.
[51] *U.S. v. Instant Checkmate, Inc.*, No. 3:14-cv-00675-H-JMA (S.D. Cal. Apr. 1, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3221/instant-checkmate-inc; *U.S. v. Infotrack Information Servs., Inc.*, No. 1:14-cv-02054 (N.D. Ill. Mar. 24, 2014), *available at*

One theme I am stressing in our privacy program is the connection between the sale of sensitive data and fraud. In fact, we often discover in our fraud cases that the scammers used highly sensitive data bought from another company, often a data broker – including Social Security and bank account numbers – to trick or steal from consumers.[54] This data goes well beyond the usual lead lists we've been seeing for years.

Two recent cases illustrate this growing problem. Data brokers Leap Lab and Sequoia One both were able to purchase the payday loan applications of financial strapped consumers – which included names, addresses, phone numbers, employers, SSNs, and bank account numbers – and sell them to scam artists who used the data to withdraw millions of dollars from consumers' accounts.[55] Sequoia also operated its own payday loan websites as a means of obtaining this sensitive data. These types of cases reveal a very troubling trend and help to answer the question we so often hear in privacy – "where's the harm?"

---

https://www.ftc.gov/enforcement/cases-proceedings/122-3092/infotrack-information-services-inc-et-al; *U.S. v. Telecheck Servs., Inc.*, No. 1:14-cv-00062 (D.D.C. Jan. 16, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3183/telecheck-services-inc; *U.S. v. Certegy Check Servs., Inc.*, No. 1:13-cv-01247 (D.D.C. Aug. 15, 2013), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3184/certegy-check-services-inc.

[52] *See, e.g., U.S. v. Yelp, Inc.*, No. 3:14-cv-04163 (N.D. Cal. filed Sept. 16, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3066/yelp-inc; *U.S. v. TinyCo, Inc.*, No. 3:14-cv-04164 (N.D. Cal. filed Sept. 16, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3209/tinyco-inc.

[53] To date, we have brought almost forty cases against companies that violated the framework, including thirteen this past August. *See* https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework.

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

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

Finally, in the last two years, the FTC has hosted workshops and released influential reports about trends and privacy concerns in today's marketplace. These include last year's "Spring Privacy Series" to examine mobile device tracking in retail stores,[56] predictive scoring models used for marketing,[57] and health apps and devices,[58] as well as our May 2014 report on data brokers.[59]

In addition, last fall, we hosted a workshop entitled *Big Data: A Tool for Inclusion or Exclusion?*[60] 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. And in January, we issued a staff report recommending best practices for the Internet of Things.[61]

More policy work is in the pipeline. Later this month, we'll host a workshop to examine the growing use of online lead generation in various industries, including consumer lending and education.[62] The goal is to highlight best practices for entities that generate and sell consumer leads so they can avoid becoming a Leap Lab or Sequoia One, in the crosshairs of the FTC. In November, we'll host a workshop on cross-device tracking to examine the various ways that

---

[56] FTC Seminar, *Spring Privacy Series: Mobile Device Tracking* (Feb. 19, 2014), *available at* https://www.ftc.gov/news-events/events-calendar/2014/02/spring-privacy-series-mobile-device-tracking.
[57] FTC Seminar, *Spring Privacy Series: Alternative Scoring Products* (Mar. 19, 2014), *available at* https://www.ftc.gov/news-events/events-calendar/2014/03/spring-privacy-series-alternative-scoring-products.
[58] FTC Seminar, *Spring Privacy Series: Consumer Generated and Controlled Health Data* (May 7, 2014), *available at* https://www.ftc.gov/news-events/events-calendar/2014/05/spring-privacy-series-consumer-generated-controlled-health-data.
[59] 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.
[60] 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.
[61] 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.
[62] 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.

companies now track consumers across multiple devices, and not just within one device.[63] And in January, we will host a conference called PrivacyCon to examine cutting-edge research and trends in protecting consumer privacy and security.[64]

II. Conclusion

As you can see, keeping pace with the digital revolution occurring in the marketplace is keeping us very busy. While these rapid changes have provided many benefits to consumers and businesses alike, the FTC will continue to take action whenever necessary to promote compliance and deter the growth of harmful trends. Thank you for having me here today – I look forward to your questions.

[63] FTC Workshop, *Cross Device Tracking* (Nov. 16, 2015), *available at* https://www.ftc.gov/news-events/events-calendar/2015/11/cross-device-tracking.
[64] *See* FTC Press Release, *FTC Announces PrivacyCon, Issues Call to Whitehat Researchers and Academics for Presentations* (Aug. 28, 2015), *available at* https://www.ftc.gov/news-events/press-releases/2015/08/ftc-announces-privacycon-issues-call-whitehat-researchers.